Bijlage checklist (stap 3 specificeren dienst/product)

Functionaliteit

		standaardbeleid
1.1	Beschrijf de huidige functionaliteit	zie intake
1.2	Beschrijf de gewenste functionaliteit	zie intake
1.3	Welke afdelingen maken gebruiken van deze service of willen er gebruik van maken	
1.4	Wanneer (tijdstippen) moet deze service beschikbaar zijn?	
1.5	Op welke locaties wordt de service gebruikt?	
1.6	Welke beschikbaarheid (per jaar) is gewenst?	
1.7	Is er een noodprocedure beschikbaar voor als de service niet werkt. Kun je zonder deze service je werk doen?	
1.8	Wat is de relatie met andere services?	
1.9	Hoe kritisch is deze functionaliteit binnen de organisatie?	

Techniek

2.1	Wat zijn de eisen voor gebruiker- en rechtenbeheer?	
2.2	Hoeveel werkplekken zijn er nodig?	
2.3	Is er een back-up scenario nodig en hoe ziet die er uit?	
2.4	Zijn er databases nodig (SQL of Oracle)?	
2.5	Zijn er servers nodig en hoeveel?	
2.6	Zijn er interfaces met andere applicaties nodig?	
2.7	Wat is initieel de benodigde data ruimte en hoeveel zal deze groeien in de toekomst?	
2.8	Zijn er naast de productieomgeving ook nog andere omgevingen zoals acceptatie en test noodzakelijk?	
2.9	Is er hardware noodzakelijk die niet past binnen de huidige architectuur?	

Organisatie

3.1	Hoeveel personen gaan er gebruik maken van deze service (specifiek het aantal concurrent gebruikers en de verwachtte groei)?	
3.2	Is er een leverancier nodig om de service op te starten en onderhouden?	
3.3	Is er een projectmanager bij de ontwikkeling van deze service betrokken?	
3.4	Wie zorgt voor de functionele ondersteuning / beheer van deze service?	

3.5	Is er gebruikerstraining nodig?	
3.6	Is er een uiterste datum voor wanneer deze service beschikbaar moet zijn?	

Beveiliging

4.1	Is de standaard beveiliging voldoende voor deze service?	
4.2	Is er wetgeving van toepassing?	
4.3	Moet back-up data bewaard worden en voor hoelang? Moet dat beveiligd gebeuren?	
4.4	Wat is de impact en risico als alle data verloren gaat?	

De onderstaande onderdelen worden samen ingevuld met de ICT-leverancier

ICT Service

5.1	Welk deel van deze service wordt door de leverancier geleverd?	
5.2	Welke ondersteuning wordt er van de leverancier verwacht?	
5.3	Wie wordt door de leverancier benaderd over deze dienst?	
5.4	Welke afspraken moeten er worden gemaakt met andere leverancier(s)?	
5.5	Wie is de producteigenaar van deze dienst?	
5.6	Wie bepaalt of de leverancier zijn afspraken nakomt?	
5.7	Moet er periodiek onderhoud gepleegd worden?	
5.8	Past deze service binnen de huidige informatiearchitectuur	
5.9	Is er binnen de gemeente training nodig om deze service te ondersteunen?	

Voorstel

6.1	Wie werkt voorstel uit?	
6.2	Hoe rapporteren we over deze service?	
6.3	Datum goedkeuring	

Eis/Wens	Product of dienst
Eis	
Eis	
Wens	
Wens	
Eis	
Eis	
Wens	
Wens	
Eis	
Eis	
Wens	
Wens	
Eis	
Eis	
Eis	

Eis*	*afhankelijk van type applicaties
Wens	
Eis	
Eis	
Eis	
Eis	
Eis	
Eis	
Eis	
Eis	
Eis	
Eis	

Checklist Programma van eisen nieuwe softw

NAAM SOFTWAREPRODUCT:

	Compatibiliteit	Eis/Wens
Techniek	Browser; MS Edge Chromium / Google Chrome	Eis
	Office 2016/365	Eis
	Responsive behave (schaalbaar obv device)	Wens
	Meergemeentenfunctionaliteit (toevoegen andere gemeente)	Wens
	ICT werkplek/voorzieningen	
	indien van toepassing: werkomgeving Citrix (Citrix tenzij)	Eis
	Type software	
	SaaS oplossing	Eis
	App	Wens
	Toevoegen nieuwe functionaliteiten mogelijk (...tenzij)	Wens
	Ontsluiting	
	Azure AD ontsluiting (inlogproc)	Eis
	--> Single Sign on	Eis
	Beschikbaarheid vanuit elk device en internet toegang --> mfa --> tenzij wettelijk niet toegestaan	Wens
	Responsive behave (schaalbaar obv device)	Wens
	Mfa of Two way auth, tenzij in de werkomgeving	Eis
Koppelingen	**Koppelvlakken**	
	Koppelvlak inrichting obv Two way SSL (certificaat)	Eis
	API's[2] tbv PowerBI	Eis
	Financieel pakket (Key2Financien)	
	API Kadaster LV [2]	
	API BAG LV [2]	
	API BRK Basisregistratie Kadaster LV [2]	
	API WOZ LV [2]	
	Archief functie aanwezig (beheer van archief) óf koppeling JoinZD	Eis*
	--> indien nodig archief vernietiging na 7 jaren	Wens
	Datadistributie gemeentelijk (BRP)	
	NHR [2]	
	mailen namens @westerwolde.nl	
	Informatiebeveiliging	
	Beschikbaarheid 24/7/365 (98%)	Eis
	Opleveren van SLA en DAP (dossier afspraken en procedures)	Eis
	Aanwezige backup- en restoreprocedure	Eis
	[2] Tbv; API's; ikv LV bevraging: voldoen aan de 4 API specificaties tbv bevraging 4 API spcificaties beschikbaar voor overheidsspecificaties	Eis
	BIO compliancy:	

Kwalitatieve eiser	IT-functionaliteiten verlenen vanuit robuuste en beveiligde systeemketen door CSP	Eis
	Dataprotectie met de classificatie BBN2 of hoger beschermen met cryptografische maatregelen. (Data op transport) (MAILFUNCTIE ED)	Eis
	Gearchiveerde data behoort technologieonafhankelijk, raadpleegbaar, onveranderbaar en integer te worden opgeslagen en op aanwijzen van eigenaar(klant) te kunnen worden vernietigd.	Eis
	Gebruikers horen alleen toegang te verkrijgen tot IT-diensten en data waarvoor zij specifiek bevoegd zijn	Eis
	Onderlinge koppelvlakken in de keten van de CSC naar de CSP behoren te worden bewaakt en beheerst om datalekken te beperken	Eis
	Logbestanden waarin gebruikersactiviteiten, uitzonderingen en informatiebeveiligings gebeurtenissen plaatsvinden behoren te worden gemaakt, bewaard en regelmatig beoordeeld	Eis
	Aanwezigheid van een test- en productieomgeving	
Kwalitatieve eisen	**Privacy**	
	Voldoen aan de AVG	Eis
	Opleveren van een verwerkersovereenkomst	Eis
	Data ontsloten vanaf moderne datacenters binnen EER (Europa)	Eis
	Beeindiging dienstverlening dient de data kosteloos te worden teruggeleverd aan de gemeente in een te importeren formaat voor een nieuwe oplossing	Eis
	NEN norm	

ıare

Softwareproduct

Te regelen; Acceptatiecriteria GRID

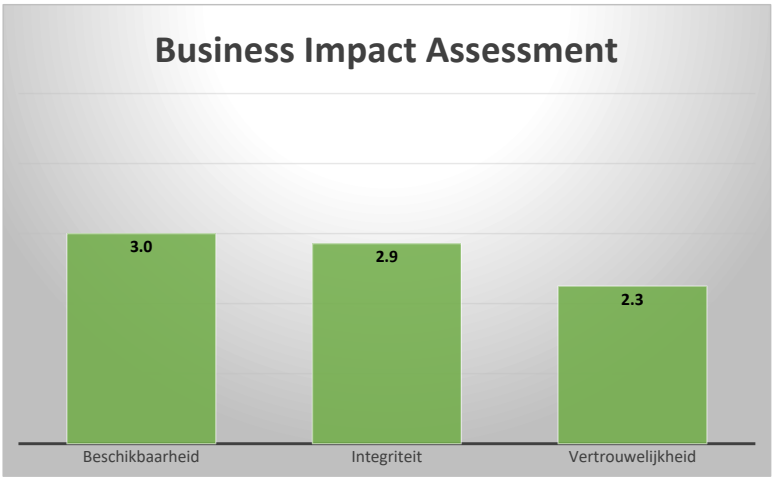
*afhankelijk van type applicaties

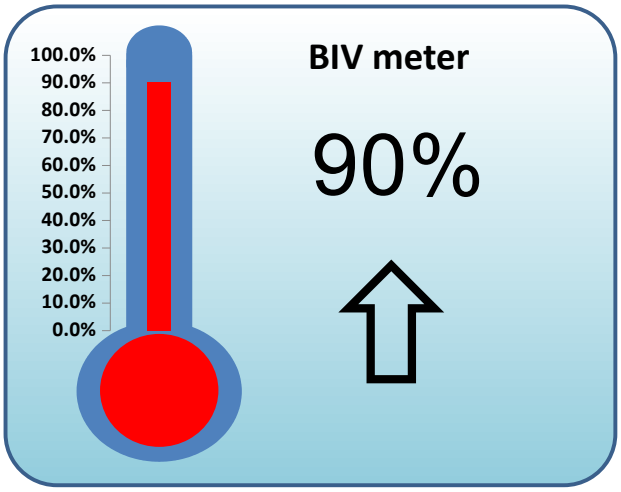
BAG altijd

Inkoop? Prestatie-eis?

OTAP procedure

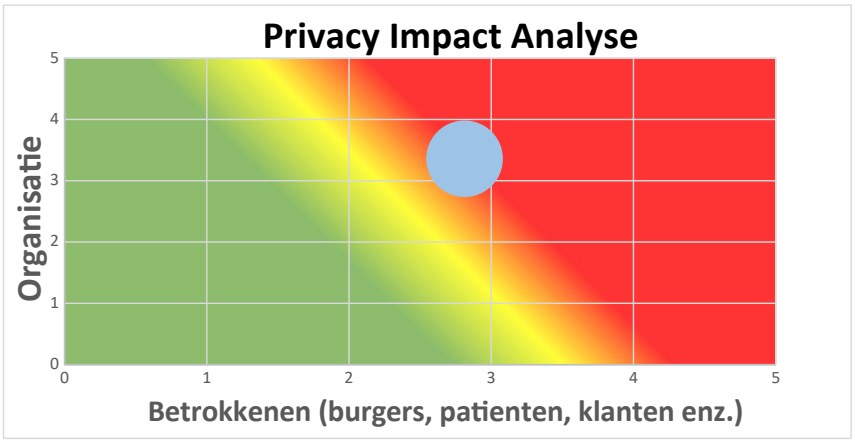
Dashboard BIA en PIA

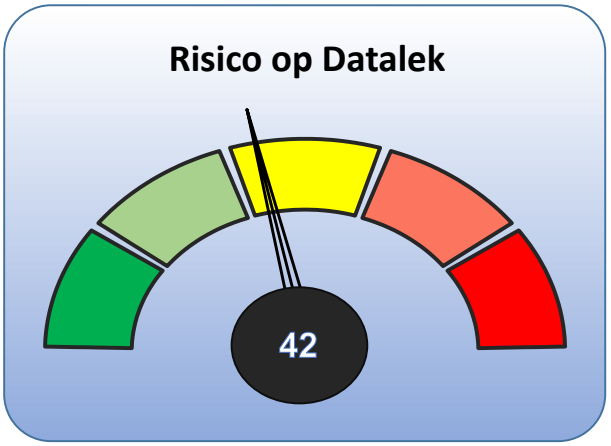


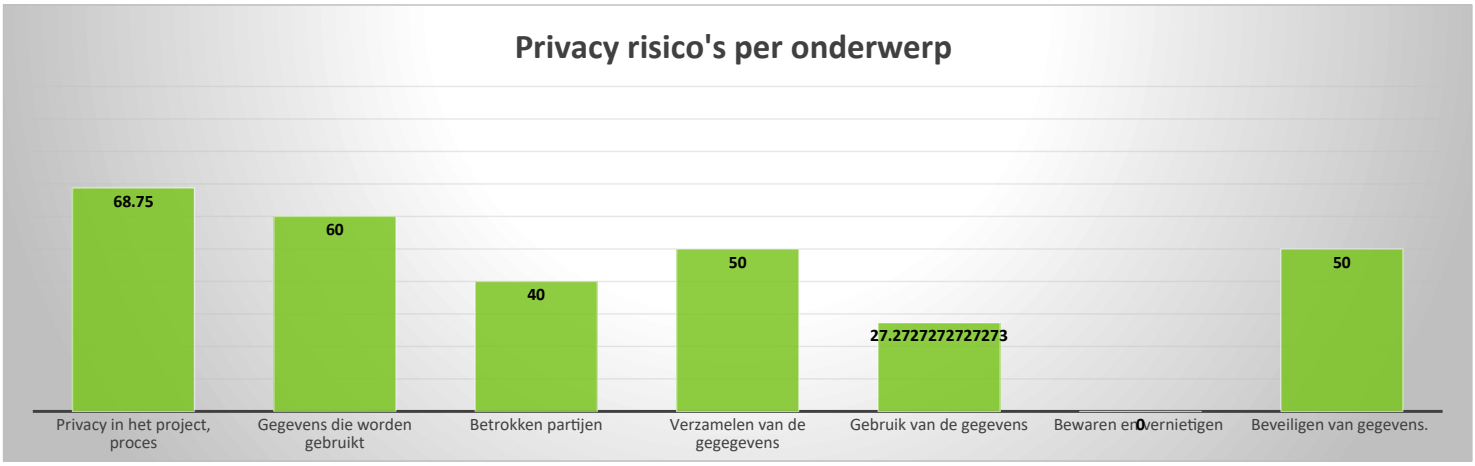


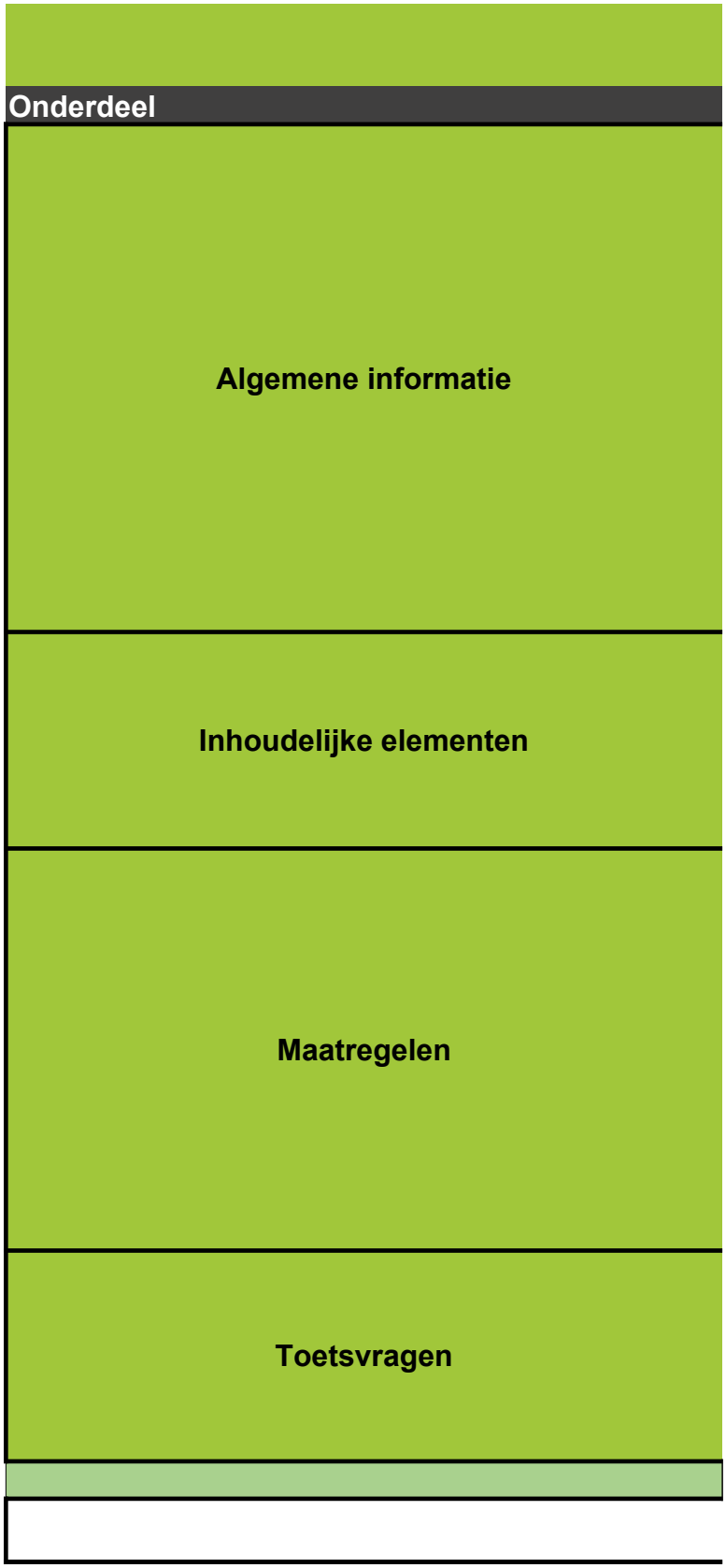
Maximale Uitvals Duur	MUD
De maximale uitvalsduur (MUD) is de tijd het informatiemiddel on-beschikbaar maar zijn door een calamiteit.	
De geaccepteerde maximale uitvalsduur is:	<1 uur

Maximale Verlies van Gegevens	MVG
Het maximale verlies van gegevens (MGV) is de tijd die besteedt is aan gegevensinvoer of arbeid die redelijkerwijs verloren mag gaan bij het terugvallen op een 1e back-up (of een generatie terug).	
Het geaccepteerde maximale verlies van (productie)gegevens is:	<1 uur








Onderdeel
Algemene informatie
Inhoudelijke elementen
Maatregelen
Toetsvragen

Onderstaande informatie over het bedrijfsproces, verwerking of applicatie g
opgenomen worden in het Register van de Verwerkingsactiviteiten.

Vragen
Naam van het proces / systeem
Beschrijf de aard van het proces / systeem
Wat is de aard van de gegevens die worden verwerkt?
Persoonsgegevens
Financiele gegevens
Kritische bedrijfsgegevens
Relevante wetgeving
Aantal afdelingen die afhankelijk zijn van het proces / systeem
Aantal personen die afhankelijk zijn van het systeem
Zijn er externe partijen afhankelijk?
Gemiste inkomsten door uitval
Beschrijving van de verwerkingsdoeleinden
Beschrijving van het keuzeproject of doorlopen stappen tot nu toe
Te verwerken persoonsgegevens
Verwerkers
Ontvangers
Bewaartermijn
Geef een overzicht van de getroffen organisatorische en technische maatregelen. Het kan zijn maatregelen al ingericht zijn voor andere processen. Controleer dan of die maatregelen voldoende effectief zullen zijn voor dit proces/verwerking.
Is de verwerking/ het project besproken in het CAB?
Wat is de impact en samenhang mbt de bestaande ICT infrastructuur?
Overzicht te treffen / getroffen maatregelen
Is de Functionaris voor gegevensbescherming betrokken bij de PIA, en zo ja, wat is het gegeven advies?
Advies van de FG
Worden maatregelen beheerd?
Overige opmerkingen
Documenteer dit document, samen met de aanvullende inf
de verwerkingsverantwoordelijke dusdanig da

jeven een beeld van de achtergrond van de vraag. De informatie kan
Antwoord
Facilitair, I(CT) moderne veilige werkplek (SP/M365) Ja Weet niet Ja gehele organisatie gehele organisatie Ja onbekend
ja.nee
niet betrokken /positief /negatief advies nee / ja, namelijk…
formatie, advies van de FG en verdere besluitvorming door at deze informatie kan dienen als naslagwerk.

Business Impact Assessment

Beschikbaarheid		Slechts 1 optie per regel invullen!					Score tussen
Onderwerpen	Vraag	0	1	2	3	Opmerkingen / verklaring	0 - 3
Wet en regelgeving	Zijn er wettelijke beschikbaarheidseisen?	> 1 maand / geen			2 dagen of minder		3
Wet en regelgeving	Zijn er interne eisen?				2 dagen of minder		3
Wet en regelgeving	Zijn externe partijen afhankelijk van het proces / systeem en bestaan er in de keten eisen?				2 dagen of minder		3
Directie schade	Hoe ernstig zijn de directe gevolgen voor de bedrijfsvoering wanneer het proces of systeem niet beschikbaar is voor een bepaalde periode?				Merkbare storing voor externe partrijen en groot aantal medewerkers		3
Directie schade	Hoe groot zijn de directe gevolgen voor de bedrijfsvoering wanneer het proces / systeem niet beschikbaar is voor een periode?				Merkbare storing voor externe partrijen en groot aantal medewerkers		3
Imagoschade / verlies van vertrouwen	Wat is de imago schade voor de organisatie wanneer het proces / systeem niet beschikbaar is?				Landelijk negatieve aandacht		3
Management	Wat zijn de gevolgen voor de besluitvorming door beleidsmedewerkers en management?	Geen					0
Overall Score						BBN3	3.0
Gemiste Omzet	Wat mist de organisatie aan inkomsten wanneer het proces / systeem niet beschikbaar is?						onbekend
Loonkosten							#VALUE!
Financiele gevolgen							**#VALUE!**

Business Impact Analyse

Item	Integriteit Vraag	0	Slechts 1 optie per regel invullen! 1	2	3	Opmerkingen / verklaring	Score tussen 0 - 3
Wet en regelgeving	Zijn er wettelijke integritetseisen?				99% juistheid		3
Wet en regelgeving	Zijn er interne eisen?				99% juistheid		3
Wet- en regelgeving	Wat is het effect op de naleving van wettelijke, voorgeschreven of contractuele verplichtingen wanneer het informatiemiddel niet beschikt over betrouwbare informatie?				tijdelijk stilleggen bedrijfsvoering >5 dagen		3
Directie schade	Hoe groot zijn de directe gevolgen voor de bedrijfsvoering wanneer het proces / systeem integriteitsproblemen heeft?				tijdelijk stilleggen bedrijfsvoering >5 dagen		3
Verlies van vertrouwen/ imagoschade	Wat zijn de gevolgen van incorrecte informatie (foutieve invoer of ongeautoriseerde invoer) voor het vertrouwen van het personeel, de klant en het publiek (imago) van de organisatie?				Landelijk negatieve aandacht		3
Management beslissingen	Hoe schadelijk zijn foutieve beslissingen op basis van incorrecte informatie (foutieve invoer of ongeautoriseerde invoer) uit het proces of informatiemiddel?				tijdelijk stilleggen bedrijfsvoering >5 dagen		3
Aansprakelijkheid (financieel risico)	Welke gevolgen heeft de incorrecte informatie (foutieve invoer of ongeautoriseerde invoer) voor juridische en contractuele verplichtingen?	€ - €					0
Moraal van de medewerkers	Wat is het effect op de moraal van de medewerkers wanneer de informatie uit het proces of informatiemiddel niet juist, volledig of tijdig is?			Medewerkers raken gefrustreerd over de fouten in de data.			2
Additionele kosten	Wat is het mogelijke effect van eventuele additionele kosten die kunnen ontstaan als gevolg van het niet juist, tijdig of volledig zijn van informatie.	€ - €					0
Overall Score						BBN3	2.9
Maximale Aansprakelijkheid (financieel risico)							€ -

Business Impact Analyse

maximale additionele kosten	€	-
Financiele gevolgen	**€**	**-**

Item	Vertrouwelijk Vraag	0	1	2	3	Opmerkingen / verklaring	Score tussen 0 - 3
Directe schade	Hoe ernstig zijn de directe gevolgen voor de bedrijfsvoering wanneer de vertrouwelijkheid van het proces niet kan worden geborgd.				Uitlekken van kritische gegevens of bijzondere persoonsgegevens		3
Directe schade	Hoe ernstig zijn de directe gevolgen voor de betrokkene wanneer de vertrouwelijkheid van het proces / systeem niet kan worden gewaarborgd?			reputatieschade of directe materiele schade			2
Verlies van vertrouwen/ imagoschade	Wat zijn de gevolgen van openbaarmaking van informatie voor het vertrouwen van de klant en het publiek (imago) in de organisatie?			Regionaal negatieve aandacht			2
Aansprakelijkheid	Welke gevolgen heeft openbaarmaking van informatie. Dit in de vorm van claims of andere juridische consequenties.						0
Moraal van de medewerkers	Wat is het effect op de moraal van de medewerkers als vertrouwelijke of gevoelige [financiële, persoonlijke, bijzondere] informatie in handen komt van ongeautoriseerde derden?			Medewerkers raken gefrustreerd over de fouten in de data.			2
Financiele herstelschade	Financiele herstelschade						0
Overall Score						BBN3	2.3
Maximale Aansprakelijkheid (financieel risico)						€	-
maximale additionele kosten						€	-
Maximale financiele gevolgen						**€**	**-**

Privacy Impact Assessment

ID	Vraag	In deze kolom uitleggen wat de situatie is en het eventuele risico	Keuze		Advies
1. Project, proces of de gegevensuitwisseling					
1.1	Is er sprake van het verwerken van persoonsgegevens?		○ Ja	○ Nee	Ga verder.
1.2	Is het duidelijk wie verantwoordelijk is voor de verwerking van de gegevens?		○ Ja	○ Nee	Ga verder.
1.3	Verwerkt je organisatie de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie? Ofwel: Treedt je organisatie op als verwerker?		○ Ja	○ Nee	Bepaal wie (bedrijfsonderdeel, persoon) binnen je organisatie de verwerkingsverantwoordelijke is.
1.4	Is het duidelijk wie na afloop van het project, proces of gegevensuitwisseling verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen?		○ Ja	○ Nee	Het risico bestaat dat de maatregelen in de toekomst niet meer worden gevolgd of niet meer passen bij de situatie.
1.5	Is het doel van de verwerking van persoonsgegevens voldoende SMART omschreven?		○ Ja	○ Nee	Een SMART omschreven doelstelling is essentieel voor het maken van keuzes voor het inrichten van een kwalitatief goede gegevensverwerking. Bovendien loopt je organisatie compliance risico's als het doel niet voldoende precies is omschreven. (Art. 5 AVG)

1.6	**Is er sprake van:**				
1.6.1	Het gebruik van nieuwe technologie?		○ Ja	○ Nee	Je loopt verhoogde risico's, de impact van je project op de betrokkenen en de wijze waarop deze gaan reageren is moeilijk in te schatten. Dit kan leiden tot verhoogde kans op imagoschade, verstoring van de bedrijfscontinuïteit, en acties door handhavers en toezichthouders.
1.6.2	Het gebruik van technologie die bij het publiek vragen of weerstand op kan roepen?		○ Ja	○ Nee	Je loopt verhoogde risico's, de impact van je project op de betrokkenen en de wijze waarop deze gaan reageren is moeilijk in te schatten. Dit kan leiden tot verhoogde kans op imagoschade, verstoring van de bedrijfscontinuïteit, en acties door handhavers en toezichthouders.
1.6.3	De invoering van bestaande technologie in nieuwe context?		○ Ja	○ Nee	Je loopt verhoogde risico's, de impact van je project op de betrokkenen en de wijze waarop deze gaan reageren is moeilijk in te schatten. Dit kan leiden tot verhoogde kans op imagoschade, verstoring van de bedrijfscontinuïteit, en acties door handhavers en toezichthouders.
1.6.4	(Andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?		○ Ja	○ Nee	Je loopt verhoogde risico's, de impact van je project op de betrokkenen en de wijze waarop deze gaan reageren is moeilijk in te schatten. Dit kan leiden tot verhoogde kans op imagoschade, verstoring van de bedrijfscontinuïteit, en acties door handhavers en toezichthouders.
1.6.5	Een nieuwe verwerking van persoonsgegevens		○ Ja	○ Nee	Ga verder.
1.6.6	Het verzamelen van meer of andere persoonsgegevens dan voorheen of een nieuwe manier van verzamelen.		○ Ja	○ Nee	Je risicoprofiel verandert. Je wordt geadviseerd een compliance check uit te voeren. Dergelijke projecten vragen om een goede beoordeling van de consequenties op het gebied van privacy.
1.6.7	Gebruik van al verzamelde gegevens voor een nieuw doel of een nieuwe manier van gebruiken.		○ Ja	○ Nee	Ga verder.
1.7	Heb je op alle bovenstaande t/m 1.6.7 "nee" geantwoord?		○ Ja	○ Nee	Ga verder.
1.8	Is er (naast de AVG) wet en regelgeving ten aanzien van persoonsgegevens waar het project, proces of gegevensuitwisseling mee te maken heeft?		○ Ja	○ Nee	Je loopt een verhoogd risico. Hoe meer wet- en regelgeving hoe hoger het risico dat je hieraan niet voldoet. Een grote hoeveelheid wet- en regelgeving duidt tevens op het maatschappelijk belang dat wordt gehecht aan het onderwerp. Je wordt geadviseerd de van toepassing zijnde wet- en regelgeving in kaart te brengen en de (privacy) consequenties inzichtelijk te maken.

1.9	Zijn er veel maatschappelijke belanghebbenden?		○ Ja	○ Nee	Ga verder.
1.10	Zijn er bij veel partijen betrokken bij de uitvoering van het project, proces of gegevensuitwisseling?		○ Ja	○ Nee	Je loopt een verhoogd risico. Het risico bestaat dat niet alle partijen zorgvuldig met gegevens omgaan die tijdens het project worden verzameld. Ook bestaat het risico dat de partijen de risico's en de inspanning die nodig is om deze te verminderen anders inschatten.
1.11	Is er een geschillenregeling/partij waar betrokkene terecht kan bij vragen of klachten?		○ Ja	○ Nee	Je loopt een verhoogd risico. Een (onafhankelijke) partij waarbij geschillen kunnen worden beslecht draagt bij aan verbetering van de voorlichting,het imago en een evenwichtige belangenbehartiging. Je wordt geadviseerd een contactpunt voor vragen en klachten aan te wijzen en waar mogelijk aan te sluiten bij geschillenregeling.
2. De Gegevens					
2.1	Zijn alle gegevens nodig om het doel te bereiken (worden er zo min mogelijk gegevens verzameld)?		○ Ja	○ Nee	Ga verder.
2.2	Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)?		○ Ja	○ Nee	
2.3	Kunnen de gegevens gebruikt worden om het gedrag, de aanwezigheid of prestaties van mensen in kaart te brengen en/of te beoordelen (ook al is dit niet het doel)?		○ Ja	○ Nee	Je loopt een verhoogd risico. Het risico bestaat dat de betrokkenen of de algemene opinie dit als een potentiële bedreiging voor hun privacy zien. Ook als de gegevens niet gevoor dit doel worden gebruikt bestaat het risico dat dit (in de toekomst) wel gebeurt. Voor de invoering van een personeelvolgsysteem is instemming van de OR nodig.
2.4	**is er sprake van**				
2.4.1	Bijzondere persoonsgegevens?		○ Ja	○ Nee	Het werken met dit type gegevens brengt een verhoogd risico van misbruik met zich mee die (potentieel grote) impactop de betrokkene heeft en vraagt daarmee om betere beveiliging. Het verwerken van deze gegevens is alleen toegestaan onder bepaalde wettelijke voorwaarden (art. 9 AVG).
2.4.2	Uniek identificerende gegevens?		○ Ja	○ Nee	

2.4.3	Wettelijk voorgeschreven persoonsnummers.		○ Ja	○ Nee	Het verwerken van een uniek bij wet voorbeschreven persoonsnummer zoals het BSN is verboden (art. 87 AVG). Je mag dit nummer alleen verwerken als je daarvoor een wettelijke basis heeft. Voor overheidsorganisaties is deze wettelijke basis neergelegd in de Wet Algemene Bepalingen Burgerservicenummer (Wabb).
2.4.4	Andere gegevens dan hiervoor beschreven waarvoor geldt dat sprake is van een (gepercipieerde) verhoogde gevoeligheid?		○ Ja	○ Nee	Het werken met dit type gegevens brengt een verhoogd risico van misbruik met zich mee die (potentieel grote) impact op de betrokkene heeft en vraagt daarmee om betere beveiliging.
2.4.5	Indien één de vragen (2.4 -2.4.4) "Ja": Kan het doel met andere gegevens worden bereikt die een verminderd risico op misbruik met zich mee brengen?		○ Ja	○ Nee	Ga verder.
2.5	Verwerk je gegevens over kwetsbare groepen of personen?		○ Ja	○ Nee	Je loopt een verhoogd risico. Indien deze gegevens worden misbruikt heeft dit negatieve beeldvorming in de publieke opinie over de organisatie tot gevolg. Je wordt geadviseerd maatregelen te treffen op een hoger beveiligingsnivea (art. 32 AVG) en betrokkenen de mogelijkheid te bieden zich aan de verwerking te onttrekken.
2.6	Gaat het om een verwerking van persoonsgegevens met meer dan 10.000 betrokkenen op jaarbasis.		○ Ja	○ Nee	Je loopt een verhoogd risico. De kans op misbruik van de gegevens wordt groter naarmate je meer gegevens verwerkt. Je wordt geadviseerd maatregelen te treffen op een hoger beveiligingsniveau (art. 32 AVG).
3. Betrokken Partijen					
3.1	Zijn er (na afronding van het project, proces of gegevensuitwisseling) bij het verzamelen om verder te verwerken van de gegevens meerdere **interne** partijen betrokken?		○ Ja	○ Nee	Je loopt een verhoogd risico. Zorg voor duidelijke beschrijving van taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: - Beveiliging van gegevens. - Afhandeling van fouten. - Terugmelden van fouten. - Afstemming van het beveiligingsbeleid. - Controle. Zorg voor een duidelijke gegevensbeschrijving.
3.2	Zijn er (na afronding van het project, proces of gegevensuitwisseling) bij het verzamelen om verder verwerken van de gegevens meerdere **externe** partijen betrokken?		○ Ja	○ Nee	Je loopt een verhoogd risico. Hoe meer partijen betrokken zijn, hoe groter de kans op verlies van gegevens, onduidelijkheden in verantwoordelijkheden, het gebruik van de gegevens voor andere doelen en de kans op fouten. Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: - De beveiliging van gegevens en de afstemming daarvan tussen de partijen. - De gegevenskwaliteit. - Afhandeling van fouten. - Terugmelden van fouten. - Controle. Zorg ook voor een duidelijke gegevensbeschrijving. Leg afspraken contractueel vast.
3.3	Zijn er partijen betrokken (in het project, proces of gegevensuitwisseling of bij de verwerking) die zich niet aan een met Nederland vergelijkbare privacywetgeving hoeven te houden?		○ Ja	○ Nee	Ga verder.

3.4	Is de verstrekking van de gegevens aan derde partijen in lijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld?		○ Ja	○ Nee	Ga verder met vraag 4.1.
3.5	Worden de gegevens verkocht aan de derde partijen?		○ Ja	○ Nee	Ga verder.
4. Verzamelen van Gegevens					
4.1	Kan de manier waarop de gegevens worden verzameld worden opgevat als privacy gevoelig?		○ Ja	○ Nee	Je wordt geadviseerd na te gaan of de gegevens op een andere manier kunnen worden verzameld.
4.2	Is het doel van het verzamelen van de gegevens publiekelijk bekend of kan het publiekelijk bekend gemaakt worden?		○ Ja	○ Nee	Ga verder.
4.3	Verzamelt u de gegevens op basis van een van de grondslagen van de AVG?		○ Ja	○ Nee	Ga verder.
4.4	Is duidelijk of je de gegevens verzamelt op basis van toestemming (opt-in) of op basis van een andere grondslag(opt-out)		○ Ja	○ Nee	Ga verder.
4.4.1	Indien je toestemming aan de betrokkene vraagt (opt-in) kunnen de betrokkenen de toestemming op een later tijdstip intrekken (opt-out)?		○ Ja	○ Nee	Ga verder.
4.4.2	Is de impact van het intrekken van de toestemming groot voor de betrokkene?		○ Ja	○ Nee	Je loopt een verhoogd risico. Indien de impact van het intrekken van de toestemming groot is, is er waarschijnlijk geen sprake van een vrije wilsuiting. Je loopt daarmee een compliance risico (art. 6.1 AVG).
4.5	Vertel je tegen de betrokkene dat de gegevens worden verzameld?		○ Ja	○ Nee	Ga verder met vraag 4.5.1.
4.5.1	Indien op de vraag 4.5 " Nee": Kunnen de betrokkenen op de hoogte zijn van het verzamelen van de gegevens?		○ Ja	○ Nee	Ga verder naar vraag 4.6
4.5.2	Indien op de vraag 4.5 " Ja":: Vertelt u tegen de betrokkene waarom de gegevens worden verzameld (wat je er mee gaat doen)?		○ Ja	○ Nee	Het verstrekken van informatie over wat je met de verzamelde gegevens gaat doen draagt bij aan de transparantie en wekt vertrouwen bij de betrokkenen. Bovendien loop je een compliance risico indien de informatie niet wordt verstrekt (art. 13 AVG).

4.5.3	Indien op de vraag 4.5 " Ja": Vertelt u tegen de betrokkene aan wie de gegevens worden verstrekt (daar waar dit geen wettelijke verplichting is)?		○ Ja	○ Nee	Een betrokkene moet geïnformeerd worden over aan wie gegevens worden verstrekt. Eveneens wordt u geadviseerd om op het moment dat de gegevens worden verzameld, de betrokkenen te vertellen aan welke partijen de gegevens verstrekt zullen worden. Als laatste wordt je geadviseerd om als betrokkenen daarom vraagt hem te vertellen welke informatie wanneer aan wie is verstrekt.
4.6	Zou de betrokkene kunnen worden verrast door de verwerking (op het moment dat hij daarover wordt geïnformeerd)?		○ Ja	○ Nee	
5. Gebruik van Gegevens					
5.1	Is het gebruik van de gegevens verenigbaar of in lijn met het doel (grondslag) van het verzamelen?		○ Ja	○ Nee	Ga verder.
5.2	Worden gegevens gebruikt voor andere bedrijfsprocessen of doelen dan waar ze oorspronkelijk voor verzameld zijn?		○ Ja	○ Nee	Ga verder naar vraag 5.2.1
5.2.1	Past het doel van dit bedrijfsproces bij het oorspronkelijke doel van verzamelen? (juridisch: het mag niet onverenigbaar zijn)		○ Ja	○ Nee	Ga verder.
5.3	Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig?		○ Ja	○ Nee	Ga verder.
5.4	Worden op basis van de gegevens beslissingen genomen over de betrokkenen?				Ga verder met vraag 5.5
5.4.1	Vormen de gegevens een volledig en actueel beeld van de betrokkenen zodat een juiste beslissing genomen kan worden?		○ Ja	○ Nee	Ga verder

5.5	Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?		○ Ja	○ Nee	Je loopt een verhoogd risico dat de gegevens gebruikt worden of in de toekomst gebruikt gaan worden voor andere doeleinden dan oorspronkelijk voor verzameld (function creep). Je wordt geadviseerd maatregelen te treffen om deze zogenaamde function creep te voorkomen of onmogelijk te maken, bijvoorbeeld door het hanteren van strikte bewaartermijnen.
5.6	Worden gegevens breed verspreid binnen de organisatie?		○ Ja	○ Nee	Je loopt een verhoogd risico. Het verspreiden van gegevens binnen de organisatie verhoogt het risico dat de gegevens voor zaken gebruikt worden waar ze niet voor bedoeld zijn of in handen komen van mensen die hier niet voor geautoriseerd zijn. Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: - Beveiliging van gegevens. - Afhandeling van fouten. - Terugmelden van fouten. - Afstemming van begeleidingsbeleid. - Controle. - Zorg voor een duidelijke gegevensbeschrijving.
5.7	Worden gegevens breed verspreid buiten de organisatie?		○ Ja	○ Nee	Je loopt een verhoogd risico. Hoe meer partijen betrokken zijn, hoe groter de kans op verlies van gegevens, onduidelijkheden in verantwoordelijkheden, het gebruik van de gegevens voor andere doelen en de kans op fouten. Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: - De beveiliging van gegevens en de afstemming daarvan tussen de partijen. - De gegevenskwaliteit. - Afhandeling van fouten. - Terugmelden van fouten. - Controle. Zorg ook voor een duidelijke gegevensbeschrijving. Leg afspraken contractueel vast.
5.7.1	Is het doorgeven van de gegevens aan partijen buiten de organisatie in lijn met de verwachtingen van de betrokkene?		○ Ja	○ Nee	Ga verder.
5.8	Stelt je organisatie profielen op van de betrokkenen, al dan niet geanonimiseerd?				Ga verder met vraag 5.9
5.8.1	Indien profielen worden opgesteld, kan het profiel tot uitsluiting of stigmatisering leiden?		○ Ja ○ Ja	○ Nee ○ Nee	Ga verder.

5.9	Kunnen de betrokkenen hun gegevens inzien of daarom vragen?		○ Ja	○ Nee	Ga verder.
5.10	Kunnen de betrokkenen hun gegevens corrigeren of daarom vragen (verbeteren, aanvullen)?		○ Ja	○ Nee	Ga verder.
5.11	Kunnen de betrokkenen hun gegevens verwijderen of daarom vragen?		○ Ja	○ Nee	Ga verder.
6. Bewaren en Vernietigen					
6.1	Is een bewaartermijn voor de gegevens vastgesteld?		○ Ja	○ Nee	Ga verder.
6.2	Kunnen de gegevens na afloop van de bewaartermijn fysiek worden verwijderd (uit een bestand) of vernietigd (papier)?		○ Ja	○ Nee	Ga verder met 6.2.1
6.2.1	Zo ja, worden de gegevens na verstrijken van de bewaartermijn op zo'n manier vernietigd of verwijderd dat ze niet meer te benaderen en te gebruiken zijn?		○ Ja	○ Nee	Ga verder.
7. Beveiligen van gegevens					
7.1	Is sprake van intern geformuleerd beleid over het beveiligen van informatie?		○ Ja	○ Nee	Ga verder.

7.2	Zo ja, is duidelijk op welke wijze het project, proces of gegevensuitwisseling er voor zorg draagt dat aan de gestelde eisen in het beveiligingsbeleid voldaan gaat worden?		◉ Ja	◉ Nee	Je wordt geadviseerd tijdens het project een informatiebeveiligingsplan op te stellen met daarin beveiligingsmaatregelen / maatregelen die voor passende bescherming van de gegevens zorgen. EINDE van deze PIA VRAGENLIJST
Zie het dashboard voor een grafische weergaven van dit advies					

Overzicht bewaartermijnen (best practice)

Medische gegevens				
Document / gegevens	**Minimale bewaartermijn**	**Maximale bewaartermijn**	**Ingangsdatum bewaartermijn**	**Vastgelegd in**
Patiëntendossier (digitaal)	15 jaar	Beleid: geen vernietiging	vanaf datum vervaardiging (of zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit)	art. 7: 456 Wet op de Geneeskundige Behandelingsover eenkomst
Patiëntendossier (papier)	15 jaar	Beleid vernietiging na 30 jaar van alle gescande papieren dossiers	vanaf datum vervaardiging (of zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit)	art. 7: 456 Wet op de Geneeskundige Behandelingsover eenkomst

Financiële gegevens

Document / gegevens	Minimale bewaartermijn	Maximale bewaartermijn	Ingangsdatum bewaartermijn	Vastgelegd in
Jaarrekening, accountantsverklaring e.d.	7 jaar	Beleid geen maximale verplicht en daarom ook niet gedefinieerd	vanaf datum opstellen	BW art. 2: 394 BW
Winst- en verliesrekening	7 jaar	Beleid geen maximale verplicht en daarom ook niet gedefinieerd	vanaf datum opstellen	art. 2: 10 en 3: 15a BW
Administratie na ontbinding rechtspersoon	7 jaar	Beleid geen maximale verplicht en daarom ook niet gedefinieerd	na ontbinding	art. 2: 24 BW
Grootboek, debiteurenadministratie, crediteurenadministratie, in- en verkoopadministratie, voorraadadministratie en loonadministratie	7 jaar	Beleid geen maximale verplicht en daarom ook niet gedefinieerd	vanaf 1 januari na het opstellen	art. 52 Wet Rijksbelastingen art. 8 Douanewet
Facturen i.v.m. de omzetbelasting	7 jaar	Beleid geen maximale verplicht en daarom ook niet gedefinieerd	na opstellen c.q. ontvangst	art. 31 Uitvoeringsbeschikking omzetbelasting

Afdelingsdocumenten

Document / gegevens	Minimale bewaartermijn	Maximale bewaartermijn	Ingangsdatum bewaartermijn
Notulen, Besluiten, Rapporten Raad van Bestuur/ College van Bestuur	**Voorbeeld:** Geen minimale termijn gedefinieerd. Beleidsvoornemen is 15 jaar, voor statuten wordt dit 30 jaar.	**Voorbeeld:**Geen maximale termijn gedefinieerd. Beleidsvoornemen is 15 jaar, voor statuten wordt dit 30 jaar.	**Voorbeeld:** Per kalenderjaar vastgesteld
Niet gepubliceerd (digitaal)	**Voorbeeld:** Geen minimale bewaartermijn. Eigenaar is verantwoordelijk. De ICT beheerorganisatie zorgt dat document tot	ICT beheerorganisatie zorgt dat document tot het moment van door de eigenaar bepaalde vernietiging bewaard worden.	**Voorbeeld:**Geen bewaartermijn
Niet gepubliceerd (papier)	**Voorbeeld:** Geen minimale bewaartermijn	**Voorbeeld:** Geen maximale bewaartermijn	**Voorbeeld:** Geen bewaartermijn
Gepubliceerd (digitaal)	**Voorbeeld:** Eigenaar bepaald termijn.	**Voorbeeld:** Eigenaar bepaald termijn.	**Voorbeeld:** Na opstellen dan wel publiceren

	Personeelsgegevens		
Vastgelegd in	**Document / gegevens**	**Minimale bewaartermijn**	**Maximale bewaartermijn**
	Sollicitatiebrieven, -formulieren, correspondentie omtrent de sollicitatie, getuigschriften en verklaring omtrent gedrag		4 weken zonder toestemming, 1 jaar met toestemming van de sollicitant
Voorbeeld: Eigenaar informatie bepaald bewaartermijn.	Arbeidsovereenkomst en wijzigingen		2 jaar
Voorbeeld: Eigenaar informatie bepaald bewaartermijn.	Wijzigingen arbeidsovereenkomst		2 jaar
Voorbeeld: Eigenaar informatie bepaald bewaartermijn. Bij het publiceren van een document moet er wel een bewaartermijn worden meegegeven, waarneer dit termijn afloopt	Correspondentie over benoemingen, promotie, demotie en ontslag	2 jaar	
	Verslagen van functioneringsgesprekken	2 jaar	
	Verslaglegging in het kader Wet Verbetering Poortwachter		2 jaar
	Loonbelastingverklaringen en kopieën van identiteitsbewijzen	5 jaar	

Afspraken betreffende salaris en arbeidsvoorwaarden	7 jaar	
Burgerlijke staat werknemer	7 jaar	
VUT-regeling		2 jaar
Afspraken inzake werk OR		2 jaar
Loonbeslagen		tot opheffing
Gegevens betreffende etniciteit en herkomst	5 jaar	
Identiteitspapieren van van derden ingeleende vreemdelingen waarvoor een tewerkstellingsvergunning is verleend	5 jaar	

Ingangsdatum bewaartermijn	Vastgelegd in
na beëindiging sollicitatieprocedure	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
einde dienstverband	Art. 52 Wet Rijksbelastingen
einde dienstverband	Art. 52 Wet Rijksbelastingen
einde dienstverband	Art. 52 Wet Rijksbelastingen
einde dienstverband	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
einde dienstverband	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
einde dienstverband	Art. 23 a Uitvoeringsregeling loonbelasting

einde dienstverband	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
einde dienstverband	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
einde dienstverband	Art. 52 Wet Rijksbelastingen
einde lidmaatschap	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
einde dienstverband	Wet stimulering Arbeidsdeelnamen Minderheden - Wet Samen
afloop kalenderjaar waarin arbeid door ingeleende vreemdeling is beëindigd	Wet Arbeid Vreemdelingen

Excel Export ICO Wizard tbv Inkoopafdeling/opdrachtgev

Inkooponderdelen	Applicatieontwikkeling algemeen
Proceseis	ja
Producteis	ja
Eis voor de opdrachtgever	ja
Eis voor de opdrachtnemer	nee
Ook eisen meegeven die alleen te maken hebben met schaalgrootte	ja
Basispakket	ja
Privacy-supplement	nee
Toon BIO-O maatregelen BBN1	nee
Toon BIO-O maatregelen BBN2	nee
Toon ABDO-eisen TBB4	nee
Toon ABDO-eisen TBB3	nee
Toon ABDO-eisen TBB2	nee
Toon ABDO-eisen TBB1	nee
Aantal geselecteerde eisen	75

Nr	Naam Eis	Referentie brondocument:	Referentie code norm:	BIO-O-maatregel:
134	Classificatie van informatie	Thema Applicatieontwikk	B.03	Ja
136	Engineeringprincipes voor beveiligde systemen	Thema Applicatieontwikk	B.04	Ja
141	Business Impact Analyse (BIA)	Thema Applicatieontwikk	B.05	Ja

142	Privacy en bescherming persoonsgegevens	Thema Applicatieontwikk	B.06	Ja
151	Analyse en specificatie informatiesystemen	Thema Applicatieontwikk	U.04	
152	Analyse en specificatie informatiebeveiligingseisen	Thema Applicatieontwikk	U.05	Ja
154	Applicatie-ontwerp	Thema Applicatieontwikk	U.06	
158	Systeemacceptatietest	Thema Applicatieontwikk	U.10	Ja
253	Informatiebeveiligingsbeleid	Beveiligingsrichtlijnen W	B.01	
254	Contractmanagement	Beveiligingsrichtlijnen W	B.05	
255	Toegangsvoorzieningsmiddelen	Beveiligingsrichtlijnen W	U/TV.01	
274	Verwervingsbeleid softwarepakketten	Thema Softwarepakkette	B.01	Ja
275	Informatiebeveiligingsbeleid voor leveranciersrelaties	Thema Softwarepakkette	B.02	Ja
276	Exit-strategie	Thema Softwarepakkette	B.03	
277	Bedrijfs- en beveiligingsfuncties	Thema Softwarepakkette	B.04	
278	Cryptografie	Thema Softwarepakkette	B.05	Ja

280	Beveiligingsarchitectuur	Thema Softwarepakkette	B.06	
282	Beperkingen wijziging softwarepakket	Thema Softwarepakkette	U.02	Ja
297	Evaluatie leveranciersdienstverlening	Thema Softwarepakkette	C.01	Ja
323	Beleid voor beveiligde inrichting en onderhoud	Thema Serverplatform	B.01	Ja
325	Inrichtingsprincipes voor serverplatform	Thema Serverplatform	B.02	Ja
334	Serverplatform-architectuur	Thema Serverplatform	B.03	
337	Malwareprotectie	Thema Serverplatform	U.03	Ja
351	Technische kwetsbaarhedenbeheer	Thema Serverplatform	U.04	Ja
357	Beheer op afstand	Thema Serverplatform	U.06	
368	Evaluatierichtlijn servers en serverplatforms	Thema Serverplatform	C.01	
383	Beheerorganisatie servers en serverplatforms	Thema Serverplatform	C.06	
387	Beleid en procedures voor informatietransport	Thema Communicatievo	B.01	
393	Overeenkomst vooren informatietransport	Thema Communicatievo	B.02	

394	Cryptografiebeleid voor communicatie	Thema Communicatievo	B.03	Ja
396	Organisatiestructuur netwerkbeheer	Thema Communicatievo	B.04	
397	Richtlijnen voor netwerkbeveiliging	Thema Communicatievo	U.01	
410	Vertrouwelijkheids- en of geheimhoudingsovereenkomst	Thema Communicatievo	U.04	
412	Beveiliging van netwerkdiensten	Thema Communicatievo	U.05	Ja
446	Netwerk beveiligingsarchitectuur	Thema Communicatievo	U.17	
447	Naleving richtlijn netwerkbeheer en evaluaties	Thema Communicatievo	C.01	
448	Compliance-toets netwerkbeveiliging	Thema Communicatievo	C.02	
612	Toegangbeveiligingsbeleid	Thema Toegangsbeveili	B.01	
626	Eigenaarschap	Thema Toegangsbeveili	B.02	
628	Beveiligingsfunctie	Thema Toegangsbeveili	B.03	
631	Cryptografie	Thema Toegangsbeveili	B.04	Ja
640	Beveiligingsorganisatie	Thema Toegangsbeveili	B.05	

688	Speciale toegangsrechtenbeheer	Thema Toegangsbeveili	U.06	Ja
691	Functiescheiding	Thema Toegangsbeveili	U.07	Ja
695	Geheime authenticatie-informatie	Thema Toegangsbeveili	U.08	
705	Autorisatie	Thema Toegangsbeveili	U.09	Ja
718	Autorisatievoorzieningen	Thema Toegangsbeveili	U.10	
724	Beoordelingsprocedure	Thema Toegangsbeveili	C.01	
727	Beoordeling toegangsrechten	Thema Toegangsbeveili	C.02	Ja
730	Logging en monitoring	Thema Toegangsbeveili	C.03	Ja
733	Beheersorganisatie toegangsbeveiliging	Thema Toegangsbeveili	C.04	
754	Exit-strategie	Thema Clouddiensten	B.03	
757	Risicomanagement	Thema Clouddiensten	B.06	
765	Risico-assessment	Thema Clouddiensten	U.02	
767	Herstelfunctie voor data en clouddiensten	Thema Clouddiensten	U.04	

768	Dataprotectie	Thema Clouddiensten	U.05	
769	Dataretentie en gegevensvernietiging	Thema Clouddiensten	U.06	Ja
772	Malware-protectie	Thema Clouddiensten	U.09	Ja
774	Toegang IT-diensten en data	Thema Clouddiensten	U.10	Ja
776	Cryptoservices	Thema Clouddiensten	U.11	Ja
779	Koppelvlakken	Thema Clouddiensten	U.12	Ja
786	Logging en monitoring	Thema Clouddiensten	U.15	Ja
788	Clouddienstenarchitectuur	Thema Clouddiensten	U.16	
930	n.v.t.	n.v.t.	n.v.t.	Ja
945	Beleid middlewarecomponenten	Thema Middleware	B.01	
946	Beleid informatietransport	Thema Middleware	B.02	
947	Data en privacy	Thema Middleware	B.03	
951	Toegang tot middlewarefunctionaliteit	Thema Middleware	U.03	Ja

952	Hardening middlewarecomponenten	Thema Middleware	U.04	
953	Configuratie middlewarecomponenten	Thema Middleware	U.05	
958	Dataherstel	Thema Middleware	U.10	Ja
959	Schonen data en media	Thema Middleware	U.11	Ja
961	Capaciteitsbeheer	Thema Middleware	U.13	
962	Evaluatie-richtlijnen	Thema Middleware	C.01	
966	Monitoren gebruikers- en beheerdersactiviteiten	Thema Middleware	C.05	

Samengesteld door
Organisatie
Datum

Samenvatting eis:
Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.
Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.
De BIA behoort te worden uitgevoerd vanuit verschillende perspectieven, zich te richten op verschillende scenario’s en vast te stellen welke impact de aspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid hebben op de organisatie.

Bij het ontwikkelen van applicaties behoren privacy en bescherming van persoonsgegevens, voor zover van toepassing, te worden gewaarborgd volgens relevante wet- en regelgeving.
De functionele eisen die verband houden met nieuwe informatiesystemen of voor uitbreiding van bestaande informatiesystemen behoren te worden geanalyseerd en gespecificeerd.
De beveiligingseisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen en voor uitbreidingen van bestaande informatiesystemen.
Het applicatieontwerp behoort gebaseerd te zijn op informatie, die is verkregen uit verschillende invalhoeken, zoals: business-vereisten en reviews, omgevingsanalyse en (specifieke) beveiliging.
Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.
De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.
In een contract met een derde partij voor de uitbestede levering of beheer van een web-applicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.
Het toegangsvoorzieningsbeleid formuleert, op basis van eisen en wensen van de organisatie, richtlijnen voor de organisatorische en technische inrichting (ontwerp) van de processen en middelen, waarmee de toegang en het gebruik van ICT-diensten wordt gereguleerd.
Voor het verwerven van software behoren regels te worden vastgesteld en op verwervingsactiviteiten binnen de organisatie te worden toegepast.
Met de leverancier behoren de informatiebeveiligingseisen en een periodieke actualisering daarvan te worden overeengekomen.
In de overeenkomst tussen de klant en leverancier behoort een exit-strategie te zijn opgenomen, waarbij zowel een aantal bepalingen over exit zijn opgenomen, als een aantal condities die aanleiding kunnen geven tot een exit.
De noodzakelijke bedrijfs- en beveiligingsfuncties binnen het veranderingsgebied behoren te worden vastgesteld met organisatorische en technisch uitgangspunten.
Ter bescherming van de communicatie en opslag van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.

De klant behoort het architectuurlandschap in kaart te hebben gebracht waarin het softwarepakket geïntegreerd moet worden en beveiligingsprincipes te hebben ontwikkeld.
Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd.
De klant behoort regelmatig de dienstverlening van softwarepakketleveranciers te monitoren, te beoordelen en te auditen.
Voor het beveiligd inrichten en onderhouden van het serverplatform behoren regels te worden vastgesteld en binnen de organisatie te worden toegepast.
Principes voor het inrichten van beveiligde servers behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het inrichten van servers.
De functionele eisen, beveiligingseisen en architectuurvoorschriften van het serverplatform zijn in samenhang in een architectuurdocument vastgelegd.
Ter bescherming tegen malware behoren beheersmaatregelen voor preventie, detectie en herstel te worden geïmplementeerd, in combinatie met het stimuleren van een passend bewustzijn van gebruikers.
Informatie over technische serverkwetsbaarheden[1] behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden dient te worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.
Richtlijnen en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van beheer op afstand van servers.
Richtlijnen behoren te worden vastgesteld om de implementatie en beveiliging van servers en besturingssystemen te controleren waarbij de bevindingen tijdig aan het management worden gerapporteerd.
Binnen de beheerorganisatie is een beveiligingsfunctionaris benoemd die de organisatie ondersteunt in de vorm van het bewaken van beveiligingsbeleid en die inzicht verschaft in de inrichting van de servers en het serverplatform.
Ter bescherming van het informatietransport, dat via allerlei soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.
Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.

Ter bescherming van informatie behoort een cryptografiebeleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
In het beleid behoort te zijn vastgesteld dat een centrale organisatiestructuur gebruikt wordt voor het beheren van netwerken (onder andere Local Area Network (LAN) en Virtual Local Area Network (VLAN)) en zo veel mogelijk van de hardware en softwarecomponenten daarvan.
Organisaties behoren hun netwerken te beveiligen met richtlijnen voor ontwerp, implementatie en beheer.
Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie, betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.
Beveiligingsmechanismen, dienstverleningsniveaus en beheereisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
De beveiligingsarchitectuur behoort de samenhang van het netwerk te beschrijven en structuur te bieden in de beveiligingsmaatregelen, gebaseerd op het vigerende bedrijfsbeleid, de leidende principes en de geldende normen en standaarden.
Richtlijnen voor de naleving van het netwerkbeveiligingsbeleid behoren periodiek getoetst en geëvalueerd te worden.
De naleving van een, conform het beveiligingsbeleid, veilige inrichting van netwerk(diensten), behoort periodiek gecontroleerd te worden en de resultaten behoren gerapporteerd te worden aan het verantwoordelijke management (compliancy-toetsen).
Een toegangsbeveiligingsbeleid behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en informatiebeveiligingseisen.
Het eigenaarschap en de verantwoordelijkheden voor logische toegangsbeveiligingssystemen en de verantwoordelijkheden voor fysieke toegangsbeveiligingssystemen behoort te zijn vastgelegd.
Een gespecialiseerde beveiligingsfunctie dient te zijn vastgesteld die verantwoordelijk is voor het bevorderen van toegangsbeveiliging binnen de gehele organisatie.
Ter bescherming van authenticatie-informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
De organisatie moet een beveiligingsorganisatie gedefinieerd hebben waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden (TVB) van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.

Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.
Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigingen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.
Toegang (autorisatie) tot informatie en systeemfuncties van toepassingen behoren te worden beperkt in overeenstemming met het toegangsbeveiligingsbeleid.
Ter ondersteuning van autorisatiebeheer moeten binnen de daartoe in aanmerking komende applicaties technische autorisatievoorzieningen, zoals: een personeelsregistratiesysteem, een autorisatiebeheersysteem en autorisatiefaciliteiten, beschikbaar zijn.
Om het gebruik van toegangsbeveiligingsvoorzieningen te (kunnen) controleren, behoren er procedures te zijn vastgesteld.
Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
Log-bestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
De eigenaar van het toegangsbeveiligingssysteem en toegangsmiddelen dient een beheersingsorganisatie ingericht hebben waarin de processtructuur, de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen zijn vastgesteld.
In de clouddienstenovereenkomst tussen de CSP en CSC behoort een exitstrategie te zijn opgenomen waarbij zowel een aantal bepalingen6 over exit zijn opgenomen, als een aantal condities6 die aanleiding kunnen geven tot een exit.
De CSP behoort de organisatie en verantwoordelijkheden voor het risicomanagementproces voor de beveiliging van clouddiensten te hebben opgezet en onderhouden.
De CSP behoort een risico-assessment uit te voeren, bestaande uit een risico-analyse en risico-evaluatie met de criteria en de doelstelling voor clouddiensten van de CSP.
De herstelfunctie van de data en clouddiensten, gericht op ondersteuning van bedrijfsprocessen, behoort te worden gefaciliteerd met infrastructuur en IT-diensten, die robuust zijn en periodiek worden getest.

Data (‘op transport’, ‘in verwerking’ en ‘in rust’) met de classificatie BBN2 of hoger behoort te worden beschermd met cryptografische maatregelen en te voldoen aan Nederlandse wetgeving.
Gearchiveerde data behoort gedurende de overeengekomen bewaartermijn, technologie-onafhankelijk, raadpleegbaar, onveranderbaar en integer te worden opgeslagen en op aanwijzing van de CSC/data-eigenaar te kunnen worden vernietigd.
Ter bescherming tegen malware behoren beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel in combinatie met een passend bewustzijn van de gebruikers.
Gebruikers behoren alleen toegang te krijgen tot IT-diensten en data waarvoor zij specifiek bevoegd zijn.
Gevoelige data van CSC’s behoort conform het overeengekomen beleid inzake cryptografische maatregelen tijdens transport via netwerken en bij opslag bij CSP te zijn versleuteld
De onderlinge netwerkconnecties (koppelvlakken) in de keten van de CSC naar de CSP behoren te worden bewaakt en beheerst om de risico’s van datalekken te beperken.
Logbestanden waarin gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiliging gebeurtenissen worden geregistreerd, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
De clouddienstenarchitectuur specificeert de samenhang en beveiliging van de services en de interconnectie tussen de CSC en de CSP en biedt transparantie en overzicht van randvoorwaardelijke omgevingsparameters, voor zowel de opzet, de levering en de portabiliteit van CSC-data.
Voor het inkooponderdeel Mobiele apparatuur en Telewerken zijn (nog) geen basiseisen opgenomen. Als echter ook gekozen wordt voor het tonen van BIO-O maatregelen en/of ABDO-supplementen, volgen hier de maatregelen uit resp. de BIO en de ABDO die te maken hebben met dit inkooponderdeel.
De leverancier behoort in overeenstemming met een overeengekomen middlewarecomponentenbeleid adequate maatregelen, zoals classificatie, te treffen om deze diensten te kunnen leveren.
Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.
Er behoort ter bescherming van bedrijfs- en persoonlijke data, beleid te zijn geformuleerd voor verwerking van data, tenminste voor: de vertrouwelijkheid en versleuteling van data, voor transformatie en aggregatie, voor toegang en privacy, classificatie en labelen en bescherming tegen verlies van gegevens.
Het toewijzen en gebruik van speciale toegangsrechten tot de middlewarefunctionaliteiten en speciale systeemhulpmiddelen behoren te worden beperkt en beheerst.

Voor het beveiligen van middlewarecomponenten behoren overbodige functies en ongeoorloofde toegang te worden uitgeschakeld.
De leverancier heeft conform richtlijnen en procedures de middlewarecomponenten geconfigureerd.
Regelmatig behoren back-upkopieën van informatie te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.
Media behoren op een veilige en beveiligde manier te worden verwijderd en geschoond als ze niet langer nodig zijn, overeenkomstig formele procedures.
Het gebruik van middelen behoort te worden gemonitord en beoordeeld, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.
Evaluatie-richtlijnen behoren te zijn vastgesteld om de implementatie en beveiliging van middlewarefunctionaliteiten te controleren, waarbij tekortkomingen tijdig aan het management worden gerapporteerd.
De organisatie reviewt en analyseert regelmatig de logbestanden om onjuist gebruik en verdachte activiteiten aan middlewarefunctionaliteiten vast te stellen en bevindingen aan het management te rapporteren.

5.1.2e en 5.1.2e	opgegeven inkooponderdelen. beveiligingsniveaus zijn altijd maatwerk. substituut voor eigen risicoafweging.
Gemeente Westerwolde	
PvE	
23-2-2024	Source tool voor Risicoanalyse.

Gebaseerd op: (ISO27002-paragraaf, of ander framework)	**Relevante standaard PToLU-lijst Forum Standaardisatie:**	**Verificatie methode(n):**
BIO 2019: 8.2.1.		Interne controle.
BIO 2019: 14.2.1, 14.2.5.		Overleg bewijsstukken en/of Verklaring.
SoGP 2018: IR2.2, BIO 2019 14.2.7.1.		Interne controle.

BIO 2019: 18.1.4.		Interne controle.
CIP-netwerk		Interne controle.
BIO 2019: 14.1.1.		Interne controle.
SoGP 2018: SD2.2		Interne controle.
BIO 2019: 14.2.9.		Interne controle.
Beveiligingsrichtlijnen WEB-applicaties: B.01		Overleg bewijsstukken en/of verklaring
Beveiligingsrichtlijnen WEB-applicaties: B.05		Interne controle, Overleg bewijsstukken.
Beveiligingsrichtlijnen WEB-applicaties: U/TV.01		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 14.2.1.		Overleg bewijsstukken en/of Verklaring.
BIO 2019: 15.1.1.		Overleg bewijsstukken en/of Verklaring.
CIP-netwerk		Overleg bewijsstukken en/of Verklaring.
CIP-netwerk		Overleg bewijsstukken en/of Verklaring.
BIO 2019: 10.1.1.		Overleg bewijsstukken en/of Verklaring.

CIP-netwerk		Overleg bewijsstukken en/of Verklaring.
ISO 27002 2017: 14.2.4, BIO 2019: 14.1.1.		Overleg bewijsstukken.
BIO 2019: 15.2.1.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 14.2.1.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 14.2.1, 14.2.5.		Overleg bewijsstukken en/of Verklaring.
NIST SP 800-53 Rev. 5 2020: PL-8		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 12.2.1.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 12.6.1.	STIX en TAXII (uitwisseling van cyberdreigingsinformatie)	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.
BIO 2019: 6.2.2.		Interne controle, Overleg bewijsstukken of Verklaring.
ISO 27002 2017: 10.10.2		Interne controle, Overleg bewijsstukken of Verklaring.
CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 13.2.1.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 13.2.2.		Interne controle.

BIO 2019: 10.1.1.		Interne controle, Overleg bewijsstukken of Verklaring.
BSI 200-2 2017: 4.2		Interne controle, Overleg bewijsstukken of Verklaring.
CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 13.2.4.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 13.1.2.		Interne controle, Overleg bewijsstukken of Verklaring.
CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.
CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.
CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 9.1.1.		Interne controle, Overleg bewijsstukken of Verklaring.
ISO 27002 2017: 8.1.1 ISO 27002 2017: 8.1.2 SoGP 2018: PM1.2		Interne controle, Overleg bewijsstukken of Verklaring.
SoGP 2018: SM2.1		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 10.1.1.		Interne controle, Overleg bewijsstukken of Verklaring.
ISO 27001 2017: 5.3		Interne controle, Overleg bewijsstukken of Verklaring.

BIO 2019: 9.2.3, 9.4.1.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 6.1.2.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 9.2.4.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 9.4.1.		Overleg bewijsstukken en/of Testen.
CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.
CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 9.2.5.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 12.4.1.		Interne controle, Overleg bewijsstukken of Verklaring.
CIP-netwerk		Interne controle.
CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.
ISO 27005 2018: 7.4		Interne controle, Overleg bewijsstukken of Verklaring.
ISO 27005 2018: 8.1		Interne controle, Overleg bewijsstukken of Verklaring.
CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.

ISO 27040 2016: 6.3.2.1	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam)	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.
CIP-netwerk, BIO 2019: 18.1.3.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 12.2.1.		Overleg bewijsstukken en/of Verklaring.
BIO 2019: 9.1.2.		Interne controle, Overleg bewijsstukken of Verklaring.
CIP-netwerk, BIO 2019: 10.1.1, 10.1.2.	* TLS, HTTPS en HSTS (beveiligde verbinding)	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.
CIP-netwerk, BIO 2019: 13.1.2.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 12.4.1.		Interne controle, Overleg bewijsstukken of Verklaring.
CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.
n.v.t.		n.v.t.
CIP-netwerk.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 13.2.1.		Interne controle, Overleg bewijsstukken of Verklaring.
ITU-T Part 5 2012: 8.5		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 9.2.3, 9.4.4		Interne controle, Overleg bewijsstukken of Verklaring.

ISO 27040 2016: 6.4.5		Interne controle, Overleg bewijsstukken of Verklaring.
SoGP 2018: SY2		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 12.3.1.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 8.3.1, 8.3.2.		Interne controle, Overleg bewijsstukken of Verklaring.
BIO 2019: 12.1.3.		Interne controle, Overleg bewijsstukken of Verklaring.
CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.
ISO 27002 2017: 12.4.1		Interne controle, Overleg bewijsstukken of Verklaring.

Toelichting:	Mitigeert risico nummer:
	24
	5
	5

	31
	12
	2
	38
	5
	5
	5
	5
	5
	3
	184
	28
	35

	14
	10
	28
	5
	10
	10
	6
	11
	26
	10
	39
	31
	49

	35
	27
	27
	19
	8
	27
	1
	1
	19
	2
	19
	35
	2

	20
	20
	21
	21
	21
	19
	21
	39
	19
	49
	1
	1
	49

	38
	33
	6
	21
	31
	27
	39
	10
	24
	31
	24
	21

	245
	246
	3
	18
	254
	1
	14

Mitigeert risico omschrijving:	**Mitigeert risico nummer:**
Onduidelijkheid over classificatie en bevoegdheden.	31
Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	28
Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	28

Onveilig versturen van gevoelige informatie.	131
Fouten als gevolg van wijzigingen in andere systemen.	51
Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.	3
Wetgeving over het gebruik van cryptografie.	52
Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	11
Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26
Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	1
Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	6
Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	182
Onvoldoende aandacht voor beveiliging binnen projecten.	28
Het niet beschikken over een overeengekomen leidraad/globale manier van aanpak bij beëindiging van leverancierscontracten.	
Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	185
Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	186

Systemen worden niet gebruikt waarvoor ze bedoeld zijn.	28
Uitval van systemen door configuratiefouten.	11
Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	201
Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	159
Uitval van systemen door configuratiefouten.	27
Uitval van systemen door configuratiefouten.	27
Toegang tot informatie wordt geblokkeerd.	26
Uitval van systemen door softwarefouten.	26
Misbruik van kwetsbaarheden in applicaties of hardware.	49
Uitval van systemen door configuratiefouten.	26
Incidenten worden niet tijdig opgepakt.	181
Onveilig versturen van gevoelige informatie.	100
Niet beschikbaar zijn van diensten van derden.	101

Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	102
Misbruiken van zwakheden in netwerkbeveiliging.	49
Misbruiken van zwakheden in netwerkbeveiliging.	49
Misbruik van andermans identiteit.	24
Aanvallen via systemen die niet in eigen beheer zijn.	28
Misbruiken van zwakheden in netwerkbeveiliging.	28
Gebrek aan sturing op informatiebeveiliging vanuit de directie.	2
Gebrek aan sturing op informatiebeveiliging vanuit de directie.	2
Misbruik van andermans identiteit.	20
Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.	12
Misbruik van andermans identiteit.	20
Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	57
Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.	58

Misbruik van speciale bevoegdheden.	65
Misbruik van speciale bevoegdheden.	21
Onterecht hebben van rechten.	67
Onterecht hebben van rechten.	68
Onterecht hebben van rechten.	69
Misbruik van andermans identiteit.	20
Onterecht hebben van rechten.	72
Incidenten worden niet tijdig opgepakt.	40
Misbruik van andermans identiteit.	20
Niet beschikbaar zijn van diensten van derden.	50
Gebrek aan sturing op informatiebeveiliging vanuit de directie.	209
Gebrek aan sturing op informatiebeveiliging vanuit de directie.	216
Niet beschikbaar zijn van diensten van derden.	40

Wetgeving over het gebruik van cryptografie.	219
Informatieverlies door verlopen van houdbaarheid van opslagwijze.	220
Toegang tot informatie wordt geblokkeerd.	26
Onterecht hebben van rechten.	224
Onveilig versturen van gevoelige informatie.	35
Misbruiken van zwakheden in netwerkbeveiliging.	6
Incidenten worden niet tijdig opgepakt.	40
Uitval van systemen door configuratiefouten.	19
Onduidelijkheid over classificatie en bevoegdheden.	28
Onveilig versturen van gevoelige informatie.	32
Onduidelijkheid over classificatie en bevoegdheden.	31
Onterecht hebben van rechten.	244

Elke niet-noodzakelijke functie van een systeem biedt extra kansen en mogelijkheden voor fouten en misbruik, waardoor de beschikbaarheid, integriteit en vertrouwelijkheid van de data in verminderde mate is	
Als de instellingen van systeemfuncties niet volgens configuratierichtlijnen plaatsvindt, is onvoorspelbaar gedrag van componenten mogelijk, waardoor uitval van functies en datalekken kunnen ontstaan.	
Onvoldoende aandacht voor beveiliging binnen projecten.	33
Verlies van mobiele apparatuur en opslagmedia.	25
Als de toename van de aantallen berichten niet wordt bewaakt of in relatie wordt gebracht met de afgesproken en beschikbare capaciteit, kan de continuïteit van het berichtenverkeer voor alle	
Gebrek aan sturing op informatiebeveiliging vanuit de directie.	2
Systemen worden niet gebruikt waarvoor ze bedoeld zijn.	20

Mitigeert risico omschrijving:	**Mitigeert risico nummer:**
Onveilig versturen van gevoelige informatie.	128
Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	129
Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	130

Betrokkenen van wie of over wie persoonsgegevens gaan, leiden schade door ongeoorloofde of onbedoelde toegang tot persoonsgegevens, ongewenst vernietigen,	
Kwijtraken van belangrijke kennis bij niet beschikbaar zijn van medewerkers.	138
Onvoldoende aandacht voor beveiliging binnen projecten.	5
Ketenafhankelijke data (-bestanden) input/output uit systemen	53
Uitval van systemen door softwarefouten.	144
Misbruik van kwetsbaarheden in applicaties of hardware.	
Gebrek aan sturing op informatiebeveiliging vanuit de directie.	49
Toegang tot informatie wordt geblokkeerd.	
Onvoldoende mogelijkheid om sturing te geven aan het verwerven van softwarepakketten.	
Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	183
Datalekken en de continuïteit niet kunnen waarborgen.	
Onvoldoende mogelijkheid om sturing te geven aan de effectieve en betrouwbare inrichting van cryptografische beheersmaatregelen binnen	

Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	187
Uitval van systemen door softwarefouten.	189
De leverancier levert niet hetgeen is opgenomen in de overeenkomst.	
Onvoldoende mogelijkheden om sturing te geven aan de effectieve en betrouwbare inrichting van een serverplatform en hierover een verantwoordingsrapportage te laten	
Misbruiken van zwakheden in netwerkbeveiliging.	51
Misbruiken van zwakheden in netwerkbeveiliging.	51
Misbruik van kwetsbaarheden in applicaties of hardware.	39
Misbruik van kwetsbaarheden in applicaties of hardware.	51
Niet beschikbaar zijn van diensten van derden.	167
Misbruik van kwetsbaarheden in applicaties of hardware.	176
De beheersorganisatie is niet effectief ingericht waardoor servers en serverplatforms onvoldoende zijn beveiligd.	
Onvoldoende mogelijkheden om sturing te geven aan informatietransport en sturing te geven aan inconsistenties in het uitvoeren van procedures en beheersmaatregelen over	
Niet helder is welke partij verantwoordelijk gesteld kan worden bij het niet halen van het gewenste beveiligingsniveau voor het transporteren van informatie over netwerken.	

Onvoldoende mogelijkheid om sturing te geven aan de effectieve en betrouwbare inrichting van cryptografische beheersmaatregelen binnen netwerken en	
Niet beschikbaar zijn van diensten van derden.	103
Niet beschikbaar zijn van diensten van derden.	104
Onduidelijkheid over classificatie en bevoegdheden.	31
Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	49
Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	120
Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.	3
Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.	3
Misbruik van speciale bevoegdheden.	26
Fouten als gevolg van wijzigingen in andere systemen.	14
Misbruik van speciale bevoegdheden.	26
Als door ontoereikend cryptografiebeleid geheime authenticatie-informatie ontrafeld kan worden, dan is de vertrouwelijkheid en integriteit van data niet te garanderen.	
Het informatiebeveiligingsbeleid komt niet effectief tot uitvoering.	

Personen die zonder aantoonbare redenen toegang hebben tot bedrijfsobjecten kunnen schade aan de bedrijfsbelangen veroorzaken.	
Onterecht hebben van rechten.	66
Er kan misbruik van gegevens door onbevoegden worden gemaakt.	
Door het niet beperken van toegang tot informatie en functies van toepassingssystemen kunnen ongewenste wijzigingen in een informatiesysteem worden	
Er treedt vervuiling op bij het autorisatiebeheer, die mogelijk in onvoldoende mate of niet tijdig wordt gesignaleerd, waardoor onbevoegden toegang hebben tot	
Misbruik van speciale bevoegdheden.	26
Door het ontbreken van controle op toegangsrechten worden afwijkingen in het autorisatieproces niet gesignaleerd en kan ongemerkt vervuiling optreden. Hierdoor	
Informatie voor het aanpakken van incidenten ontbreekt.	41
Misbruik van speciale bevoegdheden.	26
Software wordt niet meer ondersteund door de uitgever.	51
De getroffen beveiligingsmaatregelen liggen buiten de aanvaardbare grenzen. De clouddiensten worden onder- of overbeveiligd.	
Geen of onvoldoende zicht hebben op de risico’s die van invloed zijn op clouddiensten.	
Informatie voor het aanpakken van incidenten ontbreekt.	10

Data met de classificatie BBN2 of hoger is onvoldoende beveiligd	
De beschikbaarheid en integriteit van de data wordt aangetast gedurende archivering en langer archiveren dan noodzakelijk.	
Misbruik van kwetsbaarheden in applicaties of hardware.	53
Misbruik en verlies van (gevoelige) gegevens	
Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	225
Toegang tot informatie wordt geblokkeerd.	8
Informatie voor het aanpakken van incidenten ontbreekt.	41
Misbruik van andermans identiteit.	20
Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	238
Versturen van gevoelige informatie naar onjuiste persoon.	239
Onveilig versturen van gevoelige informatie.	32
Als onbevoegden toegang hebben tot systeemhulpmiddelen zoals beheertools, kan de beschikbaarheid, integriteit en vertrouwelijkheid van de opgeslagen data niet	

Informatieverlies door verlopen van houdbaarheid van opslagwijze.	251
Informatie op systemen bij reparatie of verwijdering.	252
Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.	3
Misbruik van speciale bevoegdheden.	259

Mitigeert risico omschrijving:	**Mitigeert risico nummer:**
Informatie wordt over- of onderbeveiligd	
Informatiebeveiligingsmaatregelen voor het implementeren van informatiesystemen zijn niet/minder effectief	
De gekozen beveiligingsmaatregelen sluiten niet aan bij de bedrijfsimpact door een beveiligingsincident.	

In het technisch ontwerp en verder zijn niet alle noodzakelijke functionele eisen meegenomen.	
Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	139
Verificatie op corrupte data(-bestanden) uit de keten.	140
Tijdens het gebruik van een informatiesysteem komen onvolkomenheden (afwijkingen op beveiligingseisen, functionele eisen, gebruikerseisen, businesseisen en business rules) voor het eerst aan het licht.	
Niet beschikbaar zijn van diensten van derden.	28
Onvoldoende mogelijkheid om sturing te geven aan leveranciersrelaties specifiek voor informatiebeveiliging.	

Onvoldoende mogelijkheid om sturing te geven op de beveiligingsmaatregelen van softwarepakketten die in de architectuur zijn opgenomen.	
Aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid van de data.	
Kwijtraken van belangrijke kennis bij niet beschikbaar zijn van medewerkers.	9
Kwijtraken van belangrijke kennis bij niet beschikbaar zijn van medewerkers.	161
Incidenten worden niet tijdig opgepakt.	53
Kwijtraken van belangrijke kennis bij niet beschikbaar zijn van medewerkers.	165
De server is onbetrouwbaar en functioneert niet naar behoren.	
De resultaten van de controle-activiteiten voldoen niet aan de verwachte eisen. Het management stuurt niet op afwijkingen.	

Het niet effectief tot uitvoering komen van het beleid.	
Aanzienlijke negatieve gevolgen voor de bedrijfsactiviteiten door het verlies van vertrouwelijkheid, integriteit en beschikbaarheid van netwerkcomponenten en/of de uitgewisselde gegevens.	
Onveilig versturen van gevoelige informatie.	18
Niet beschikbaar zijn van diensten van derden.	108
Geen sturing hebben op de netwerkbeveiliging.	
Onvoldoende aandacht voor beveiliging binnen projecten.	121
Onvoldoende aandacht voor beveiliging binnen projecten.	122
Misbruik van kwetsbaarheden in applicaties of hardware.	27
Systemen worden niet gebruikt waarvoor ze bedoeld zijn.	26
Misbruik van kwetsbaarheden in applicaties of hardware.	27

Het ontbreken van een adequate implementatie van functiescheiding kan leiden tot een verhoogde kans op fraude of misbruik van bedrijfsmiddelen bij kritische of fraudegevoelige taken. Het verstrekken van onnodige toegang vergroot het risico	
Misbruik van kwetsbaarheden in applicaties of hardware.	27
Herhaling van incidenten.	73
Misbruik van kwetsbaarheden in applicaties of hardware.	27
Kwijtraken van belangrijke kennis bij niet beschikbaar zijn van medewerkers.	206
Uitval van systemen door configuratiefouten.	11

Verificatie op corrupte data(-bestanden) uit de keten.	223
Gegevens zijn tijdens transport via netwerken en opslag te benaderen voor onbevoegden	
Aanvallen via systemen die niet in eigen beheer zijn.	31
Herhaling van incidenten.	73
Misbruik van speciale bevoegdheden.	22
Adequate sturing op geoorloofd gebruik van middlewarecomponenten is praktisch onmogelijk, waardoor schade kan ontstaan in de bedrijfsvoering.	
Adequate sturing op het informatietransport is niet mogelijk en er kunnen gemakkelijk datalekken ontstaan, zonder dat in de uitvoering sprake is van opzet of onzorgvuldig handelen.	
Versturen van gevoelige informatie naar onjuiste persoon.	240

Als data niet kan worden hersteld na storingen, diefstal, systeemuitval of calamiteiten wordt de continuïteit van de bedrijfsvoering ernstig in gevaar gebracht.	
Als opslagmedia na gebruik niet adequaat wordt geschoond of onherstelbaar wordt vernietigd, kunnen er datalekken ontstaan wanneer deze media in andere systemen wordt hergebruikt of in handen van onbevoegden terechtkomen.	
Onvoldoende aandacht voor beveiliging binnen projecten.	255
Niet kunnen vaststellen wie welke handelingen heeft uitgevoerd. Control De organisatie reviewt en analyseert regelmatig de logbestanden o	

Mitigeert risico omschrijving:	Mitigeert risico nummer:

Het ontbreken van informatiebeveiligingseisen voor nieuwe of uit te breiden informatiesystemen.	
In het applicatieontwerp ontbreekt vereiste informatie	
Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	

Uitval van systemen door hardwarefouten.	160
Onvoldoende sturing hebben op de inrichting van het serverplatform. Bedreigingen worden over het hoofd gezien.	
Verificatie op corrupte data(-bestanden) uit de keten.	164
Kwetsbaarheden in servers worden niet opgemerkt, waardoor er misbruik van gemaakt kan worden.	

Verlies van mobiele apparatuur en opslagmedia.	107
Uitval van kritische processen van de organisatie.	
Geen of onvoldoende inzicht of de richtlijnen voor het naleven van het netwerkbeveiligingsbeleid het netwerkbeveiligingsbeleid effectief toetsten.	
Afwijkingen op het beveiligingsbeleid worden niet gesignaleerd.	
Misbruiken van zwakheden in netwerkbeveiliging.	54
Misbruik van kwetsbaarheden in applicaties of hardware.	27
Misbruiken van zwakheden in netwerkbeveiliging.	56

Misbruiken van zwakheden in netwerkbeveiliging.	71
Zonder vastlegging en bewaking kan achteraf niet de juiste actie worden ondernomen en niet worden vastgesteld wie welke handelingen heeft uitgevoerd.	
Misbruiken van zwakheden in netwerkbeveiliging.	74
Het niet beschikken over een overeengekomen leidraad/globale manier van aanpak bij beëindiging van leverancierscontracten.	
Uitval van systemen door softwarefouten.	12

Malware wordt niet opgespoord en aangetroffen malware wordt niet of voldoende hersteld.	
Onveilig versturen van gevoelige informatie.	32
Zonder vastlegging en bewaking kan achteraf niet de juiste actie worden ondernomen en niet worden vastgesteld wie welke handelingen heeft uitgevoerd.	229
Slecht wachtwoordgebruik.	31
Als organisaties zich niet bewust zijn van de vergaande mogelijkheden van integratiefuncties in de middleware en niet hebben geformaliseerd welke transformaties bedrijfs-	

Onvoldoende mogelijkheden om vast te stellen of controle-activiteiten gestructureerd en binnen vastgestelde periodiek plaatsvinden.	

Mitigeert risico omschrijving:	Mitigeert risico nummer:

Bij de inrichting van servers zijn niet alle vereiste beveiligingsprincipes meegenomen.	
Malware wordt niet of te laat opgespoord en aangetroffen malware wordt niet of voldoende hersteld.	

Dienstverleners en partners zijn niet (voldoende) bekend met de actuele benodigde eisen van de organisatie voor het beschermen van informatie.	
Onvoldoende mogelijkheden om enerzijds sturing te geven aan de effectieve en betrouwbare inrichting van toegangsbeveiligingsmaatregelen en anderzijds sturing te geven aan het inrichten van de beheerorganisatie van de	
Misbruiken van zwakheden in netwerkbeveiliging.	55
Door het ontbreken van de beveiligingsfunctie is het mogelijk dat activiteiten over toegangsbeveiliging ongecoördineerd, onjuist of niet tijdig worden uitgevoerd of dat afwijkingen niet leiden tot corrigerende acties.	

Onvoldoende mogelijkheden om vast te stellen of de controle-activiteiten gestructureerd plaatsvinden.	
De beheersorganisatie is niet effectief ingericht waardoor het toegangsbeveiligingssysteem niet optimaal functioneert.	
Fouten als gevolg van wijzigingen in andere systemen.	218

Versturen van gevoelige informatie naar onjuiste persoon.	226
Afwijkingen van normaal gedrag zijn niet zichtbaar en niet te onderzoeken en herstelacties kunnen niet tijdig worden genomen.	
Onveilig versturen van gevoelige informatie.	32

Mitigeert risico omschrijving:	Inkooponderdeel	Eis gevraagd J/N
	Applicatieontwikkeling algemeen	
	Applicatieontwikkeling algemeen	
	Applicatieontwikkeling algemeen	

	Applicatieontwikkeling algemeen	
	Applicatieontwikkeling algemeen	
	Applicatieontwikkeling algemeen	
	Applicatieontwikkeling algemeen	
	Applicatieontwikkeling algemeen	
	DiGiD Applicaties	
	DiGiD Applicaties	
	DiGiD Applicaties	
	Softwarepakketten	
	Softwarepakketten	
	Softwarepakketten	
	Softwarepakketten	
	Softwarepakketten	

	Softwarepakketten	
	Softwarepakketten	
	Softwarepakketten	
	Serverplatform	
	Serverplatform	
	Serverplatform	
	Serverplatform	
	Serverplatform	
	Serverplatform	
	Serverplatform	
	Serverplatform	
	Communicatievoorzieningen	
	Communicatievoorzieningen	

	Communicatievoorzieningen	
	Communicatievoorzieningen	
	Communicatievoorzieningen	
	Communicatievoorzieningen	
	Communicatievoorzieningen	
	Communicatievoorzieningen	
	Communicatievoorzieningen	
	Communicatievoorzieningen	
	Toegangsbeveiliging	
Het bewerkstelligen dat er een verantwoordelijke is voor het toegangsbeveiligingssysteem voor een betrouwbare inrichting, dan wel ervoor	Toegangsbeveiliging	
	Toegangsbeveiliging	
	Toegangsbeveiliging	
	Toegangsbeveiliging	

	Toegangsbeveiliging	
	Toegangsbeveiliging	
	Toegangsbeveiliging	
	Toegangsbeveiliging	
	Toegangsbeveiliging	
	Toegangsbeveiliging	
	Toegangsbeveiliging	
	Toegangsbeveiliging	
	Toegangsbeveiliging	
	Toegangsbeveiliging	
	Clouddiensten	
	Clouddiensten	
	Clouddiensten	
Overschrijden van het maximale dataverlies en/of uitvalsduur.	Clouddiensten	

	Clouddiensten	
	Clouddiensten	
	Clouddiensten	
	Clouddiensten	
	Clouddiensten	
Data van of in beheer van de CSP komt via de koppelvlakken in handen van de CSP.	Clouddiensten	
	Clouddiensten	
Versturen van gevoelige informatie naar onjuiste persoon.	Clouddiensten	
	Mobiele apparatuur & telewerken	
	Middleware	
	Middleware	
	Middleware	
	Middleware	

	Middleware	
	Middleware	
	Middleware	
	Middleware	
	Middleware	
	Middleware	
	Middleware	

Als Eis/Wens	Reden niet gevraagd/geeist	Weging in RFC

Inleiding		
Kunt u een **omschrijving** geven van de ICT dienst die u heeft uitbesteed of wil gaan uitbesteden?	nvt	
Contractuele aspecten		
Is de **looptijd** van de dienstverlening concreet benoemd?	Ja	Zo ja: Wat is de looptijd van het contract?
Heeft u een mogelijkheid om de **dienstverlening** elders onder te brengen (Vendor Lock-in)?	Ja	Zo ja: Wat zijn de alternatieven?
Is in het contract duidelijk omschreven wat de dienstverlening inhoud? Dus inclusief concrete **kwaliteitseisen** en eventueel wat de consequenties zijn van meer en minder werk.	Ja	
Zijn er contractuele afspraken gemaakt over de **monitoring** van de kwaliteitseisen? Denk hierbij ook aan auditing.	Ja	
Zijn er afspraken gemaakt over de **geheimhouding**?	Ja	
Zijn er afspraken gemaakt over het melden van incidenten cq **datalekken**?	Ja	

Heeft u een clausule opgenomen over een eventuele **bedrijfsovername**?	Ja
Zijn er afspraken gemaakt over **arbitrage** en het van toepassing zijnde recht in het geval van een **dispuut**?	Ja
Zijn er afspraken gemaakt over het **beëindigen** van de overeenkomst.	Ja
Zijn er afspraken gemaakt over het terugleveren, migreren cq vernietigen van **data**? Denk hierbij ook aan de vorm waarin data wordt terug geleverd.	Ja
Is de leverancier **gecertificeerd** of heeft de leveranciers een auditverklaring. - ISO 27001/2 gecertificeerd? - ISAE3402 / T2 - Verwerkersovereenkomst?	Ja
AVG aspecten (Gehele vraag zichtbaar bij Ja)	
Is er sprake van het verwerken van **persoonsgegevens**?	Ja
data wordt of gaat worden opgeslagen?	
opslag plaats op een locatie waar dat is toegestaan? (EER / Vertrouwde landen / corporate rules / Privacy shield)	

verwerker verantwoordelijkheid draagt.	
rechten van de betrokkene.	
Vertrouwelijkheid	
Zijn er technische maatregelen getroffen om de communicatie tussen de organisatie en de leverancier te beveiligen (**encryptie**/**versleuteld**)?	Ja
Zijn er afspraken gemaakt over het **doorleveren** van gegevens? (**derden**)	Ja
Heeft de leverancier maatregelen getroffen om de informatie van de organisatie goed af te schermen/**beveiligen** op grond van RBAC / ABAC principes?	Ja
Integriteit	
Is er sprake van het **converteren** van gegevens?	Ja
Zo ja: Is er een beschrijving van het ETL proces ? (ETL staat voor Extractie Tranformatie Laden oftewel de interface)	Ja

Geeft de leverancier een verklaring over de integriteit van de bestanden en de bestandseigenschappen?	Ja
Continuïteit	
Heeft de leverancier maatregelen getroffen om de **continuïteit** te waarborgen?	Ja
Sluiten de **maatregelen** van de leverancier aan op de termijnen die aan de organisatie zijn gesteld door klanten en toezichthouders?	Ja
Wordt het **back-up** systeem en een eventuele uitwijk minimaal jaarlijks getest?	Ja
Heeft de leverancier maatregelen genomen op het gebied van intrusion detection en intrusion prevention / **SIEM**.	Ja
Worden door de leverancier andere **klanten** bediend waardoor het risico op een cyberaanval wordt vergroot. Denk hierbij bijvoorbeeld aan het hosten van een website van een politieke partij.	Ja
Heeft de leverancier maatregelen genomen op het gebied van **DDOS** beveiliging? - Heeft de leverancier maatrelgelen genomen om de vereiste beschikbaarheid te kunnen waarborgen?	Ja
- Heeft de leverancier maatrelgelen genomen om de vereiste beschikbaarheid te kunnen waarborgen?	Ja

Controleerbaarheid	
Vind er **logging** plaats op de systemen en in de applicatie van de leverancier?	Ja
Voert de leverancier periodiek **controles** (securitytest) uit zodat men enige zekerheid kan verschaffen over de weerstand tegen een eventuele cyberaanval?	Ja
Worden er door de leveranciers controles uitgevoerd zoals: '- **soc** monitoring? - periodiek **audit**s?	Ja

3 jaar	Niet voldoen aan wet en regelgeving	0	
Overheids instantie	Vendor lock-in waardoor u een slechtere onderhandelingsmogelijkheden heeft en problemen kan krijgen bij niet nakoming van de contractuele afspraken.	0	
	Wanneer de dienstverlening niet duidelijk is omschreven heeft u weinig mogelijkheden om afspraken te laten nakomen of de leverancier heeft mogelijkheden om zaken als meerwerk aan te merken wat kan	0	
	De leverancier dient zich periodiek te verantwoorden over de service level afspraken, zodat u als klant kan beoordelen of de afspraken worden negekomen.	0	
	In het geval van uitlekken van informatie heeft u geen juridische mogelijkheden om de leverancier aansprakelijk te stellen. Daarnaast kan een leverancier eerder geneigd zijn om gegevens onzorgvulidg te	0	Nee
	U kunt een boete opgelegd krijgen van de Autoriteit persoonsgegevens voor het niet of niet tijdig melden van een datalek waar u verantwoordelijk voor bent.	0	Nee

	In het geval van een bedrijfsovername kunnen nieuwe voorwaarden van toepassing worden of werkzaamheden verplaatst worden naar andere lokaties. Dit kan juridische gevolgen hebben.	0		
	In het geval van een dispuut wilt u voorkomen dat u in een ander land een procedure moet aanspannen.	0		
	U dient een exit strategie te hebben en deze te hebben afgesproken met de leverancier. Dit zodat het eenvoudiger is om afscheid te nemen van een leverancier en de werkzaamheden elders onder te	0		Ja
	Het niet maken van afspraken kan ertoe leiden dat informatie bij de leverancier blijft staan of zelfs wordt vernietigd zodat het lastig en zoniet onmogelijk wordt om een contract te beeindigen.	0		Ja
	Wanneer een leverancier een verklaring heeft van een externe auditor inzake de mate waarin zij voldoen aan beveiligs en privacy eisen dan kunt u aantonen zorgvuldig gehandeld te hebben.			Ja
			AVG gevoelig	Err:507
				Nee
				Nee

			Nee
			Nee
	Het niet beveiligen kan leiden tot het uitlekken van vertrouwelijke informatie of persoonsgegevens	0	Nee
	Het doorleveren van gegevens dient alleen te mogen wanneer daar uitdrukkelijke toestemming voor is gegeven. In het geval van persoonsgegevens kan dit ook een schending van de privacy zijn wat	0	Nee
	Uw leverancier en daarmee ook loopt hiermee een beveiligingsrisico op ongeoorloofde toegang tot de data.	0	Nee
	Er dient een beschrijving van het ETL proces te bestaan waardoor deze kan worden beheerd.		

	Het is van belang dat de kwaliteit van de data wordt gecontroleerd. Dit ter voorkoming van fouten in het primaire proces.	0	
	Het gebrek aan maatregelen kan leiden tot uitval van de dienstverlening.	0	
	Het gebrek aan maatregelen kan leiden tot uitval van de dienstverlening.	0	
	Het gebrek aan maatregelen kan leiden tot uitval van de dienstverlening.	0	
	Het gebrek aan maatregelen kan leiden tot uitval van de dienstverlening.	0	Ja
	Andere klanten kunnen leiden tot een verhoogd risiconiveau.	0	Ja
	Het gebrek aan maatregelen kan leiden tot uitval van de dienstverlening.	0	
	Het gebrek aan maatregelen kan leiden tot uitval van de dienstverlening.	0	

	Gebrek aan logging maakt analyse en incidentanalyse onmogelijk.	0	Nee
	Gebrek aan inzicht in kwetsbaarheden kan leiden tot het verstren van de bedrijfsvoering en/of het uitlekken van informatie	0	Nee
	Het gebrek aan maatregelen kan leiden tot uitval van de dienstverlening of het te laat ddetecteren van een hackpoging.	0	Nee

Versie	1.0
Beheerder	Procesmanager
Eigenaar	Procesmanagement
Bestandsnaam	Acceptatiecriteria

betreft changenummer: MS Teams / SMT

		Afspraak vooraf
In voorbereidingsfase	Intake formulier volledig ingevuld of alle gegevens zijn in Teams map beschikbaar?	Eis
	Check wetgeving/installatie voorschriften leverancier (temperatuur, aarding, luchtvoch	
	Technisch ontwerp opgesteld	
	Installatie handleiding aanwezig	
	Business Impact analyse opgesteld (IM/IB)	Eis grote change
	Privacy impact analyse uitgevoerd (IB&P)?	
In productiename	Omgeving technisch ingericht (inclusief voorzieningen tegen stroomuitval)	
	Draaiboek t.b.v. in productiename	
	Fallback plan aanwezig	
	Rollback plan aanwezig	
	Organisatie geïnformeerd	Eis
	Gebruikers opgeleid	
	Werkinstructies geschreven / aangepast	
	Vrijgave rapportage GAT opgeleverd of controle uitgevoerd door gebruiker	
	Standaard account in apparatuur of software van levenciers zijn aangepast	
	Nazorg(periode) afgesproken	
	Aanpassen standaard wachtwoorden op apparatuur leveranciers (cfm wachtwoordbeleid)	
In beheername	Functioneel beheer toegewezen en opgeleid	
	Applicatie beheer toegewezen en opgeleid	
	Technisch beheer toegewezen en opgeleid	Eis
	Check op toepassen installatievoorschriften leverancier	
	DVO, PDC of SLA opgesteld of aangepast	
	DAP / UC leverancier opgesteld of aangepast	
	Is een vorm van logging/monitoring (rapportage) noodzakelijk	
	Licentiebeheer bijgewerkt	
	Apparatuur is beschermd tegen onderbreking van nutsvoorzieningen	
	Oude infrastructuur opgeruimd	
Check testen, documenteren	Architectuur plaat applicatielandschap aangepast	
	Autorisatiematrix ingevuld	
	Technisch ontwerp (bijgewerkt naar definitieve inrichting).	
	Installatie documentatie opgeleverd of Configuratie Document	
	Back-up procedure ingeregeld en getest	
	Restore procedure ingeregeld en getest	
	Disaster Recovery ingeregeld en getest	
	A en P omgeving ingericht	
	Security Baselines toegepast (inclusief patching/hardenining)	
	Certificaatbeheer conform richtlijnen ingericht	
	CMDB en evt. softwarecatalogus gevuld	Eis

Afspraak vooraf is:
NVT (niet van toepassing)
Eis (moet opgeleverd worden)
Nee (hoeft niet opgeleverd te worden)

verantwoordelijk voor de uitvoering
aanvrager
Coordinator en/of behandelaar
Behandelaar of Architectuur Board
Behandelaar
Changecoordinator of projectleider
FG gemeente
Behandelaar
Projectleider (alleen cat 1 change)
Changecoordinator of projectleider
Changecoordinator of projectleider
Changecoordinator of projectleider
Changecoordinator of projectleider
Changecoordinator of projectleider
Projectleider
Changecoordinator of projectleider
Projectleider
Engineer
Changecoordinator of projectleider iom lijnmanager
Changecoordinator of projectleider iom lijnmanager
Changecoordinator of projectleider iom lijnmanager
Changecoordinator of projectleider
Manager klantprocessen (SLM)
Manager klantprocessen (SLM)
Changecoordinator of projectleider
Configuratie manager
Changecoordinator of projectleider
Engineer of projectleider
Architect
Bedrijfsbureau
Changecoordinator of projecteider
Changecoordinator of projecteider
Changecoordinator of projecteider
Changecoordinator of projecteider
Changecoordinator of projecteider
Changecoordinator of projecteider
Engineers
Changecoordinator of projecteider
Change Coördinator

vastleggen in / op (bij afsluiten change)
Formulier in MS Teams
MS T\eams
MS T\eams
MS T\eams
MS T\eams Formulier in MS Teams
infrastructuur
MS T\eams
MS T\eams
MS T\eams nvt nvt W:-schijf bouwblokken projectmap of Sysaid nvt nvt
Bij (laten) werken van de kennismatrix Bij (laten) werken van de kennismatrix Bij (laten) werken van de kennismatrix nvt W:-schijf W:-schijf nvt Bedrijfsbureau informeren tbv contractendatabase nvt SysAid (bij hardeschijven bijvoorbeeld)
W:-schijf W:-schijf W:-schijf bouwblokken W:-schijf bouwblokken W:-schijf bouwblokken W:-schijf bouwblokken W:-schijf bouwblokken nvt nvt nvt SysAid

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	55
Wet open overheid	Art. 5.1 lid 2 sub f	De bescherming van andere dan in het eerste lid, onderdeel c, genoemde concurrentiegevoelige bedrijfs- en fabricagegegevens	14